

94th Congress }
2d Session }

COMMITTEE PRINT

PROBLEMS ASSOCIATED WITH COMPUTER
TECHNOLOGY IN FEDERAL PROGRAMS
AND PRIVATE INDUSTRY

COMPUTER ABUSES

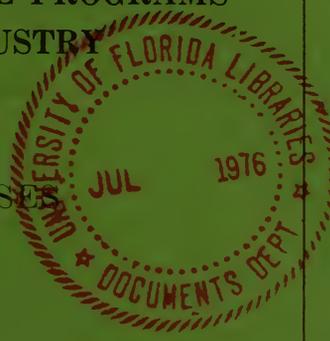
PREPARED BY THE

COMMITTEE ON GOVERNMENT OPERATIONS
UNITED STATES SENATE



JUNE 1976

Printed for the use of the Committee on Government Operations



**PROBLEMS ASSOCIATED WITH COMPUTER
TECHNOLOGY IN FEDERAL PROGRAMS
AND PRIVATE INDUSTRY**

COMPUTER ABUSES

PREPARED BY THE

**COMMITTEE ON GOVERNMENT OPERATIONS
UNITED STATES SENATE**



JUNE 1976

Printed for the use of the Committee on Government Operations

U.S. GOVERNMENT PRINTING OFFICE

72-538 O

WASHINGTON : 1976

COMMITTEE ON GOVERNMENT OPERATIONS

ABRAHAM RIBICOFF, Connecticut, *Chairman*

JOHN L. McCLELLAN, Arkansas
HENRY M. JACKSON, Washington
EDMUND S. MUSKIE, Maine
LEE METCALF, Montana
JAMES B. ALLEN, Alabama
LAWTON CHILES, Florida
SAM NUNN, Georgia
JOHN GLENN, Ohio

CHARLES H. PERCY, Illinois
JACOB K. JAVITS, New York
WILLIAM V. ROTH, JR., Delaware
BILL BROCK, Tennessee
LOWELL P. WEICKER, JR., Connecticut

RICHARD A. WEGMAN, *Chief Counsel and Staff Director*

PAUL HOFF, *Counsel*

PAUL L. LEVENTHAL, *Counsel*

ELI E. NOBLEMAN, *Counsel*

DAVID R. SCHAEFER, *Counsel*

MATTHEW SCHNEIDER, *Counsel*

FRED ASSELIN, *Investigator*

JOHN B. CHILDERS, *Chief Counsel to the Minority*

BRIAN CONBOY, *Special Counsel to the Minority*

MARILYN A. HARRIS, *Chief Clerk*

ELIZABETH A. PREAST, *Assistant Chief Clerk*

HAROLD C. ANDERSON, *Staff Editor*

CONTENTS

	Page
Memorandum from Senator Abe Ribicoff to all Members of the Senate Government Operations Committee.....	IX
Remarks of Senator Ribicoff on Computer Problems in Government, from the Congressional Record, May 10, 1976.....	1
 GAO REPORT ENTITLED "IMPROVEMENTS NEEDED IN MANAGING AUTOMATED DECISIONMAKING BY COMPUTERS THROUGHOUT THE FEDERAL GOVERNMENT," APRIL 23, 1976:	
Digest.....	12
Chapter 1. Introduction.....	15
Automated decisionmaking applications.....	15
Characteristics.....	15
Contrast with other computer applications.....	17
Chapter 2. Use of automated decisionmaking applications by Federal agencies.....	18
Information about automated decisionmaking applications used by Federal agencies.....	18
Functions supported by automated decisionmaking applications..	19
Number of automated decisionmaking applications and their impact on Federal agencies.....	19
Reasons for output of actions for manual review and evaluation..	20
An example of what automated decisionmaking applications do..	21
Chapter 3. Automated decisionmaking applications can make bad decisions.....	22
Conditions leading to bad decisions.....	22
Software problems reported.....	24
Data problems reported.....	26
Internal audits of automated decisionmaking applications.....	28
Chapter 4. Causes of bad automated decisions.....	29
Software problems.....	29
Data problems.....	34
Chapter 5. Federal management of automated decisionmaking applications.....	38
Responsibilities for ADP management in the Government.....	38
Policy actions by Federal agencies to manage automated decisionmaking applications.....	39
What agencies do.....	39
Chapter 6. Automated decisionmaking applications continue to make bad decisions until problems are corrected.....	45
Error detection.....	45
Error correction.....	45
Agency procedures for timely correction of software design problems.....	46
Chapter 7. Opinion on ways to prevent or reduce the impact of problems in automated decisionmaking applications.....	47
Possible solutions—software problems.....	47
Possible solutions—data problems.....	48
Chapter 8. Conclusions, recommendations, and agency comments.....	50
Recommendations.....	51
Agency comments.....	52
Appendix I. Letter dated November 17, 1975, from the Assistant Secretary of the Department of Health, Education, and Welfare.....	54
Appendix II. Letter dated November 28, 1975, from the Associate Deputy Administrator, Veterans Administration.....	60

Appendix III. Letter dated December 29, 1975, from the Acting Administrator of General Services.....	Page 61
Appendix IV. Letter dated January 2, 1976, from the Assistant Secretary of Defense (Comptroller).....	63
Appendix V. Internal audit reports on automated decisionmaking applications	66

ABBREVIATIONS

- ADP—Automatic Data Processing
- ASO—Aviation Supply Office
- DSA—Defense Supply Agency
- FMSO—Fleet Material Support Office
- GAO—General Accounting Office
- GSA—General Services Administration
- HEW—Department of Health, Education, and Welfare
- OMB—Office of Management and Budget
- SSA—Social Security Administration
- VA—Veterans Administration

GAO REPORT ENTITLED "COMPUTER-RELATED CRIMES IN FEDERAL PROGRAMS," APRIL 27, 1976:

Digest	73
Chapter 1. Introduction.....	74
What is a computer-related crime?.....	74
Federal managers have responsibility to establish effective controls	74
How information on crimes was gathered.....	75
Chapter 2. The nature of government computer crimes.....	76
What kinds of crimes are occurring?.....	76
How do Government crimes compare to those in the private sector?	78
Why do these crimes occur?.....	79
Chapter 3. Criminals exploited weaknesses in basic management controls	80
Inadequate separation of duties and poor physical controls are the most common weaknesses.....	80
Once designed, controls must be used.....	81
Chapter 4. Management does not place sufficient emphasis on controlling systems.....	82
Management placed priority on making systems operational rather than on controlling them.....	82
Management did not assess potential threats to systems.....	82
Chapter 5. Improvement needed in audits of system controls.....	84
Proper audits can detect weaknesses that lead to crimes.....	84
Audits of controls had not been made.....	84
Auditors should be informed of criminal activity indicating control weaknesses.....	85
Chapter 6. Conclusions and recommendations.....	86
Recommendations	86
Agency comments	87
Chapter 7. Scope of review.....	88
Appendix I. List of cases included in our review.....	89

- GAO—General Accounting Office
- ADP—Automatic Data Processing
- SRI—Stanford Research Institute

GAO REPORT ENTITLED: "MANAGERS NEED TO PROVIDE BETTER PROTECTION FOR FEDERAL AUTOMATIC DATA PROCESSING FACILITIES," MAY 10, 1976:

Digest	95
Chapter 1. Introduction.....	97
Some definitions.....	97
Responsibility for security.....	98
Scope of study.....	99

	Page
Chapter 2. Security at facilities visited was inadequate-----	100
Fire -----	101
Flood -----	104
Sabotage -----	107
Theft or misuse-----	111
Power fluctuations-----	113
Contingency planning-----	113
Chapter 3. Federal data processing security practices-----	118
Government-wide guidance-----	118
Responsibility for physical security-----	119
Guidelines should apply to all Federal installations-----	119
Chapter 4. Conclusions, agency comments, and our evaluation and recommendations -----	120
Conclusions -----	120
Agency comments and our evaluation-----	121
Recommendations -----	123
Appendix I. A concept for use in making security decisions-----	124
Risk management-----	124
Need for a risk manager-----	128
Appendix II. Summary of security areas covered-----	131
Appendix III. Letter dated March 12, 1976 from the Office of Manage- ment and Budget-----	139
Letter dated March 17, 1976 from the Department of Commerce--	142
Letter dated March 15, 1976 from the Department of Defense----	144
Letter dated March 15, 1976 from the Department of Health, Education, and Welfare-----	146
Letter dated March 12, 1976 from the Department of Transportation -----	147
Appendix IV. Action summary of "Guidelines for Automatic Data Processing Physical Security and Risk Management"-----	148
ADP—automatic data processing	
GAO—General Accounting Office	
GSA—General Services Administration	
NBS—National Bureau of Standards	
OMB—Office of Management and Budget	

Material supplied by the Science Policy Research Division of the Congressional Service, Library of Congress:

Memorandum of Louise Giovane Becker, analyst in Information Sciences, Congressional Research Service, Library of Congress. Computer and information security in the Federal Government. An Overview including selected references and Glossary for computer security FIPS PUB 39-----	153
Courtney, Robert H., Jr. Security risk assessment in electronic data processing systems. December 1975-----	181
Turn, Rein and Willis H. Ware. Privacy and security in computer systems. American scientist, v. 63, March-April 1975: 196-203----	259
Ball, Leslie and Steven D. Wood. Computer security in concentrated information systems. Arizona business, v. 23, March 1976: 23-29----	271
Browne, Peter S. Computer security—a survey. G.E. Information Services Business Division, Rockville, Md-----	279
Weiss, Harold. Computer security—an overview. Datamation, v. 20, January 1974: 42-47-----	287
Palme, Jacob. Software security. Datamation, v. 20, January 1974----	298
Marion, Larry. U.S. to require computer security. Electronics, July 25, 1974: 78, 79-----	309
Baird, Lindsay L., Jr. How to identify computer vulnerability. Bank Administration, October 1974: 16-21-----	311
Law officials warn of computer crime. New York Times, Nov. 23, 1975-----	318
Brandstad, Dennis K. Data protection through cryptography. Dimensions NBS, September 1975-----	320

	Page
Executive guide to computer security. U.S. Department of Commerce--	324
Skala, Martin. Protection for computers growing. Washington Post, Oct. 6, 1974: p. H2-----	335
Espionage in the computer business. Business week, July 28, 1975: 60-62-----	336
Kahn, David. Tapping computers. New York Times, Apr. 3, 1976: p. 27-----	341
Irwin, T. K. The new computer crooks: the intricate schemes that net millions. Washington Family weekly (Washington Star News) Apr. 7, 1974-----	343
DeWeese, J. Taylor. The trojan horse caper—and assorted other com- puter crimes. Saturday review, v. 3, Nov. 15, 1975: 10, 58-60-----	345
Allen, Brandt. Embezzler's guide to the computer. Harvard business review, v. 53, July-August 1975: 79-89-----	351
Alexander, Tom. Waiting for the great computer rip-off. Fortune, v. 90, July 1974: 143-148-----	364
Brenner, Lynn. Interest in computer security mushrooms. Journal of Commerce, May 19, 1975-----	373
Parker, Donn B. and Susan Nycum. The new criminal. Datamation, v. 20, January 1974: 56-57-----	376
Voysey, Hedley. Computers need protection against programers. New Scientist, v. 63, Aug. 22, 1974: 464-----	382
Privacy and security: twin challenges to computer technology. Dimensions/National Bureau of Standards, v. 58, July 1974: 147- 149-----	383
Nycum, Susan Hubbell. Computer abuses raise new legal problems. American Bar Association Journal, April 1975: 444-448-----	386
Stone, Robert L. EDP accounting. The Journal of American Account- ancy, February 1975: 35-39-----	393
Memorandum from Fred Asselin, investigator, to Senator Ribicoff, June 18, 1976-----	403
Wright, Robert A., "Fraud by Computer Is Averted on Coast," New York Times, December 8, 1974-----	403
Wright, Robert A., "Check for \$902,000 in Los Angeles Swindle Plan Is Cashed Here," New York Times, December 10, 1974-----	405
Baker, Erwin, "L.A. Check Security: Where Did Thief Hit?" Los Angeles Times, December 10, 1974-----	408
Getze, John, "Checks and Balances—No Plan Is Fail-Safe," Los Angeles Times, December 20, 1974-----	411
"Woman Is Given 94 Years in Plot To Bilk Los Angeles," New York Times, December 29, 1975-----	414
Hill, G. Christian, "Large Loan Swindles Spread With Reliance on Cen- tral Data Bank," Wall Street Journal, March 12, 1976-----	414
Immel, Richard A., "Sabotage, Accidents, and Fraud Cause Woes for Computer Centers," Wall Street Journal, March 22, 1971-----	419
Menkus, Belden, "Computerized Information Systems Are Vulnerable to Fraud and Embezzlement," Menkus, on Management Newsletter, Au- gust 1972-----	422
Holmes, Edith, "Error Rate for SSI Checks Hit 23.7 Percent," Computer- world, May 10, 1976-----	425
"Guard That Computer," Nation's Business, April 1971-----	427
Christensen, Kathryn, "Divorcing by Computer?" the Washington Post, May 23, 1976-----	432
Arnst, Catherine, "Vote-Card Switch Prompts Suit Challenging Outcome of Mavoral Race in Michigan," Computerworld, March 1, 1976-----	433
Upton, Molly, "Management Seen Doing Too Little To Curb DP Crime," Computerworld, March 8, 1976-----	435
Surden, Esther, "Redtape Tying up Programing of Federal Impact Aid Funding," Computerworld, April 26, 1976-----	437
French, Nancy, "Massachusetts Welfare Department Hires DPers To Pin- point Cheaters by Matching Lists," Computerworld, May 3, 1976-----	438

VII

	Page
Arnst, Catherine, "Privacy Protection Seen Backfiring on Individuals," Computerworld, May 10, 1976-----	440
Hanlon, Joe, "UK Job-Matching Plan Attacked on Privacy Grounds," Computerworld, May 9, 1976-----	441
Arnst, Catherine, "Study Sees Computerized Nations More Vulnerable to War Threats," Computerworld, May 17, 1976-----	443
French, Nancy, "Jail Suicide Blamed on Terminal Operator," Computer- world, May 17, 1976-----	444
Bride, Edward J., "Radar Wipes Out IRS Tapes; Consultant Cites Poor Ground," Computerworld, January 6, 1971-----	446
Baker, Donald P. "Theft by Computer," Washington Post, June 16, 1976---	447



Digitized by the Internet Archive
in 2013

<http://archive.org/details/prossociat00unit>

MEMORANDUM

JUNE 18, 1976.

To: All Members of the Senate Government Operations Committee.
From: Senator Abe Ribicoff, chairman.

This Senate Government Operations Committee Print was assembled in preparation for the Committee's hearings on problems associated with computer technology in federal programs and private industry. The hearings will have special focus on computer-related crimes and computer security.

A preliminary staff investigation by the Committee was begun in April of 1976. As Chairman of the Committee, I noted in Senate remarks May 10, 1976, that the staff investigation had been initiated.

In its preliminary inquiry, the Committee staff benefited from three General Accounting Office reports. The reports, which are reprinted in this Committee Print, are "Improvements Needed in Managing Automated Decisionmaking by Computers Throughout the Federal Government," dated April 23, 1976; "Computer-Related Crimes in Federal Programs," dated April 27, 1976; and "Managers Need To Provide Better Protection For Federal Automatic Data Processing Facilities," dated May 10, 1976. Each of these reports is thorough, objective and perceptive, pointing to problems in federal computer programs which are deserving of additional evaluation by the Congress.

In addition to the GAO reports, this Committee Print also includes articles selected at the Committee's request by the Science Policy Research Division of the Congressional Research Service of the Library of Congress. These articles were selected by the Library of Congress to provide the Committee with the views of experts in the field of computer technology in connection with computer abuses and computer security.

Also included in this Committee Print are articles selected by the Committee staff reflective of a broad range of computer-related problems.

Computer technology is a difficult and complicated subject for Congressional review. It is my hope that with the information contained in the Committee Print Senators will have available to them fundamental information which will be of assistance as we go forward with hearings.

COMPUTER PROBLEMS IN GOVERNMENT

[From the Congressional Record—Senate, May 10, 1976]

Mr. RIBICOFF. Mr. President, the General Accounting Office, examining computer-related crimes in Federal programs, studied 69 individual cases that together totaled more than \$2 million in losses to the Government.

The GAO inquiry revealed that computer fraud is a growing problem in both the Government and private sector and that, in many instances—no one knows how many—it is almost impossible to detect.

The name of the GAO study is "Computer-Related Crimes in Federal Programs." The study is dated April 29, 1976.

GAO obtained its information from the investigative files of the Criminal Investigations Division—CID—Command of the Army; the Navy Investigative Service—NIS—the Office of Special Investigations—OSI—of the Air Force; the Justice Department's Executive Office for U.S. Attorneys and the FBI; the Office of Investigation of the Agriculture Department; the Internal Revenue Service in Treasury; HEW's Social Security Administration; the Division of Investigation of the Interior Department; and the Investigation and Security Services of the Veterans Administration.

In the preponderance of the 69 cases, criminal prosecutions resulted.

GAO auditors cited these instances of computer crimes in Government:

A Defense Department fuel supply employee who had helped automate an accounting system introduced fraudulent payment vouchers into the system. The computer could not recognize that the transactions were fraudulent and issued checks payable to fictitious companies set up by the employee and his accomplices. These checks were sent directly to banks where the conspirators had opened accounts for the companies. The criminals then withdrew the funds from the accounts. Officials estimated the government paid this employee and his accomplices \$100,000 for goods and that were never delivered.

A supervisory clerk responsible for entering claim transactions to a computer-based social welfare system found she could introduce fictitious food stamp claims on behalf of accomplices and they would receive the benefits. She processed more than \$90,000 in claims before she was discovered through an anonymous tip.

An engineer who was no longer employed at a computer installation managed to continue using the equipment for his own purposes. Before he was discovered, he had used more than \$4,000 worth of computer time. At another installation, a programmer used a self-initiated training program to obtain the use of his agency's computer system. But instead of working on the training exercise, he was developing his own computer programs which he hoped to sell, GAO auditors said.

The manager of a computer center processing personal information stole some of this data and sold it to private firms. The private firms, none of which were authorized to have such data, used the information to promote their products. GAO said that although the Government did not lose money in this case the privacy of individuals whose data records were involved was violated.

At one large Army installation officers estimated that 80 percent of all thefts may have been computer related.

In transmitting their report to the Congress, GAO auditors said they were precluded from being more specific about individual instances of computer fraud because first, in many instances information came from raw investigative files; second, several of the cases reviewed were still open or were about to be prosecuted at the time GAO completed its inquiry; and third, persons who had perpetrated computer frauds cooperated with GAO but with the understanding that they would not be identified.

GAO auditors said most of the cases they studied did not involve sophisticated attempts to use computer technology for fraudulent purposes. Instead, GAO said, these were uncomplicated acts which were made easier because management controls over the systems involved were inadequate.

Forty-three of the 69 cases of computer-related crimes were classified by GAO as being "fraudulent record initiation." Under this category, GAO included cases in which Federal employees, or persons employed by Government contractors, deliberately falsified information from records and documents to be fed into computers. Also included in this category was the act of falsifying claims by reuse of supporting documents previously processed.

The second category of computer-related crimes is termed "unauthorized or inappropriate use of facilities and supplies." This category includes developing salable programs on Government computers, doing commercial work for outsiders on Government computers and duplicating files and selling them.

"Processing alteration or destruction" is the third category of computer-related crimes studied by GAO. This offense includes such crimes as sabotage or altering information in the files affecting pay, promotion or assignment, and bypassing existing controls to enter unauthorized changes.

The final category examined by GAO is "misappropriation of output." Included under this section is the misappropriation of returned checks.

In connection with its review of computer-related crime in the Government, GAO commissioned the Stanford Research Institute—SRI—of Menlo Park, Calif., to study similar crimes in the private sector.

GAO said the SRI report indicates the same types of crimes occur in both the public and private sectors. GAO said in both the public and private areas the majority of crimes were committed by systems users—that is, persons working with the computers being abused—but the proportion of user crimes is larger in Government.

GAO auditors said the size of the average loss in private sector crimes is higher than in the Government cases studied. In a review of 144 cases, SRI found the average loss in private business to be \$450,000.

GAO said the average loss in those Government cases in which a dollar figure was apparent was \$44,000.

GAO said the Government should improve its management controls over computers. GAO also pointed out that auditors of Government computer programs should be educated about the prevalence and types of computer crimes. GAO said that several Government computer auditors did not know about crimes which had been committed in their own programs until GAO informed them.

Another General Accounting Office study found that Navy auditors identified a computer as being incorrectly programed in 1969 but the computer was not fixed for 5 years, during which time the machine initiated unnecessary actions that cost the Navy \$3 million a year.

GAO said one of the reasons the Navy gave for the 5-year delay was that Navy officials were concerned that by correcting the computer problem they might cause budget reductions.

Another instance of computer short-comings, GAO said, could be seen in a situation in which Army computers directed the shipment of radioactive equipment without requiring the stipulated safeguards for proper handling.

These examples were cited by GAO to demonstrate problems in the Federal Government's "automated decisionmaking computers." These computers, operating without human supervision, annually initiate payments, purchases and other expenditures involving many billions of dollars in Government funds and resources and people are not required to review these actions to determine whether they are correct or not.

In its report, dated April 26, 1976, entitled "Improvements Needed in Managing Automated Decisionmaking by Computers Throughout the Federal Government," GAO concluded:

Computers in Federal departments and agencies annually issue unreviewed payments and other actions involving billions of dollars in government assets. These actions are often wrong. They can cost the government huge sums of money ; exactly how much no one knows.

It is troubling to note the extent to which these decisionmaking computers are able to decide things on their own. Computer technology is progress, of course. But people should monitor closely what these machines are up to. For all their heralded memory banks and fantastic instant recall, computers are still basically beasts of burden. They have no intelligence, except for what information people insert in them.

"Automated decisionmaking by computers" occurs when computers are programmed to make payments, purchase material and otherwise spend money and take actions without the assistance of or review by people.

In their study of automated decisionmaking computers, GAO auditors concluded that these kinds of computers initiate more than 1.7 billion payments and other actions by government a year without any person evaluating whether they are correct.

Government automated decisionmaking computers issue each year a minimum of unreviewed authorizations for payment or checks (excluding payroll) totaling \$26 billion, the GAO report said.

Unreviewed bills totaling at least \$10 billion are issued annually by automated decisionmaking computers, the GAO auditors said.

In addition, the GAO said, these same computers issue annually unreviewed requisitions, shipping orders, repair schedules and property disposal orders for material valued at \$8 billion.

GAO obtained information on 128 automated decisionmaking computer programs at the Army, Navy, Air Force, Defense Supply Agency, General Services Administration, Railroad Retirement Board, Veterans' Administration, and the Departments of Agriculture, Commerce, Housing and Urban Development, Interior, Treasury, and Health, Education, and Welfare.

The GAO auditors cited examples in which automated decision-making computers had resulted in millions of dollars of waste and, in one instance, the unauthorized handling of radioactive components for military equipment.

In 1969, the GAO report said, the Navy's own auditors found that a computer program serving the Navy Aviation Supply Office in Philadelphia was inadequately designed regarding the ability to correctly reflect demand for the purchase and repair of naval aircraft and spare parts.

The Aviation Supply Office in Philadelphia is the central manager for all the purchases and repair of aircraft and spare parts for the entire Navy. The Aviation Supply Office is under the Naval Supply Systems Command of the Department of the Navy.

The inadequacy in the automated decisionmaking computer program at the Aviation Supply Office was not corrected. The problem was noted in a GAO study issued May 21, 1974, entitled, "Better Methods Needed For Cancelling Orders For Material No Longer Required."

Again, however, the inadequacy was not corrected and the decision-making computer continued to inaccurately reflect demand for new equipment and for repairs on naval aircraft. Five years went by before the needed correction was made. "At least \$3 million in annual unnecessary costs were initiated by automated decisionmaking applications using this overstated demand data," GAO auditors said.

Design of the automated decisionmaking computers at the Aviation Supply Office was developed at the Fleet Materiel Support Command, Mechanicsburg, Pa., which also reports to the Naval Supply Systems Command in Washington.

GAO asked Navy officials why it had taken so long to correct the computer inadequacy. The GAO report said:

The reasons cited by Navy officials for the 5-year delay in initiating the modifications included:

Disagreements within the Navy on whether all canceled requisitions should result in reducing record demands,

High-priority workload at the design activity mandated by higher headquarters levels in both the Navy and the Department of Defense, and

Lack of pressure placed on the Navy command and design activity by the inventory control points since *reduced demands could result in budget reductions.* [Emphasis added.]

The Veterans' Administration—VA—uses automated decision-making computers to make monthly payments to more than 185,000 veterans in apprenticeship and other on-the-job training programs. The VA computers are supposed to be programmed to make payments at a rate that decreases every 6 months, under the assumption that an

individual veteran's pay from his employer will increase as he learns his trade.

Annually, the VA computers process about 1.4 million unreviewed checks for more than \$225 million in apprenticeship and other on-the-job training benefits. However, the data submitted to the computers was incomplete and, GAO auditors said, checks went out at the highest levels to the veterans and no progressively declining payment system was implemented. The result, GAO said, was potential overpayments of \$700,000.

Code 8 is the designation the Army gives to equipment and spare parts which have radioactive components and which, therefore, are required to be handled by authorized personnel in a stipulated manner.

GAO said it obtained from the Army Audit Agency data concerning the Army Electronics Command, Fort Monmouth, N.J., which processes each year at least 250,000 requisitions for material valued at a minimum of \$250 million. About 35 percent of the requisitions are reviewed by people, GAO said, and the remaining 65 percent are processed by automated decisionmaking computers without review by people.

The Army Audit Agency examined 86 radioactive commodities handled by this Command's automated decisionmaking computers and found that 18 of the commodities were processed not with the radioactive designation of code 8—but instead carried a code 0 rating. Code 0 means that no special controls or handling are required, GAO said.

In addition, the GAO auditors said, another 11 radioactive commodities were categorized as code 1, the code that indicates that the item is scarce, costly or highly technical—but not that it is radioactive.

GAO said the Army Audit Agency also studied the application of automated decisionmaking computer technology at five Army inventory control points. The Army auditors found the computers were often in error in deciding where material should be shipped. The result, the Army auditors showed, was an annual loss of \$900,000 in unnecessary transportation costs. In addition, a total of \$1.3 million was incurred by the Army in the early 1970's due to unnecessary inventory increases caused by errors in these same computers.

The GAO report said that a major cause of inaccurate computer tabulations in the Government is the massive amounts of information fed into the machines which lead "input preparers"—that is, computer personnel—to make mistakes.

GAO noted, for example, that the Navy Aviation Supply Office in Philadelphia receives about 10 million "transaction reports" each year, all of which are then fed into computers. Transaction reports are mainly prepared by Navy facilities that receive, store and issue aeronautical equipment.

In addition, GAO auditors estimated that during a 12-month period the VA Center in Philadelphia prepared more than 4 million documents for insertion into computers.

To insure more accurate automatic computer calculations, GAO proposed that the Government require selective or cyclical monitoring of actions directed by automated decisionmaking computers. The

GAO also recommended that outside auditors or independent design teams from elsewhere in a given agency be called in to study the design of a computer program before it is allowed to begin making automated decisions.

A third General Accounting Office study found that the Federal Government's 9,000 computers which are involved in billions of dollars in transactions and contain vast amounts of information are inadequately protected against terrorism, vandalism, program alteration, and natural disasters.

We can see the potential harm in Government's failure to adequately protect computer facilities when we consider what enormous personal tragedies would result from serious damage to the social security computerized system. Social security could not function without its computers. It is impossible to estimate the effects on millions of our elderly citizens whose livelihood depends on social security should the computers be destroyed.

But the potential threat is not limited to social security. In terms of Federal revenues, for instance, imagine the havoc that would result from the destruction of Federal tax records.

In addition, the number of veterans in this country is larger than ever before. Each of these men and women who served in the Armed Forces may be receiving, or may be entitled to receive benefits from their military service. Valuable data and records pertaining to their military service—and the benefits that accrue from that service—are on computer tapes and, in the event of catastrophe, could be lost forever.

Since 1965, responsibility for control of computer applications in the Federal Government has been shared by the General Services Administration, the Office of Management and Budget, and the Department of Commerce.

The GAO report is named "Managers Need To Provide Better Protection for Federal Automatic Data Processing Centers." It is dated May 10, 1976.

The GAO report said the total value of Government's 9,000 computers "is many billions" of dollars.

GAO said the value of some of the data which is processed on these computers such as social security records is immeasurable.

GAO auditors said:

Consequently—protecting equipment and data from unauthorized or inadvertent acts of destruction, alteration or misuse is a matter of inestimable importance,

GAO said, for example, that the National Aeronautics and Space Administration could not carry out space programs without computer applications; nor could the Federal Aviation Administration control aircraft effectively.

Computers are used to manage the more than half-billion transactions processed by the Social Security Administration and the 4 billion facts relating to the national population compiled and managed by the Bureau of the Census, GAO auditors said, adding that many other Federal agencies rely heavily on computer technology.

Catastrophic losses to Government-sponsored data processing installations such as the loss of human life, irreplaceable data and equip-

ment have occurred, GAO said. In many of these losses, GAO said, additional security measures were implemented after the event.

GAO said information on the physical security measures employed at 28 Federal data processing facilities led its auditors to conclude that Federal data processing assets and valuable data are not properly protected.

GAO recommended that to provide more security over Government automatic data processing operations, the Office of Management and Budget—OMB—should direct that management officials be appointed at Federal installations having data processing systems and that they be assigned responsibility for automatic data processing physical security and risk management.

Reflective of the amount of money Federal agencies spend on computers, GAO said, is the fact that more than \$10 billion is expended each year to buy and operate Federal data processing systems.

In concluding that security safeguards are inadequate regarding computers, GAO studied security techniques at 28 data processing installations of the Departments of the Army, Navy, Air Force, Agriculture, Transportation, State and Health, Education and Welfare and the Veterans' Administration.

Besides the 28 Federal data processing sites, GAO auditors also studied security problems identified at 23 additional Government computer installations.

In addition, GAO examined data processing security systems used at Government contractor sites, universities, private companies, a bank, and a local government.

GAO said major areas of security covered in its investigation of data processing facilities included steps taken by management to guard against threats of modification or destruction to the physical plant, personnel, computer hardware and software, and to the data being processed or stored by the computerized systems.

Eighteen of the 28 data processing installations were in the continental United States. The remaining 10 were abroad.

Among its findings that computer installations are not properly protected, GAO noted that—

Fourteen installations had combustible paper supplies or magnetic tape files which were stored in computer rooms which exposed systems to losses from fire.

Three installations had computers which were in use in areas where only portable fire extinguishers were available.

One installation's computers were in operation where no portable fire extinguishers were available.

Twelve installations had computers which were in use above raised flooring without periodically cleaning below such flooring, constituting a fire hazard.

Six installations had computers which were in operation where master electrical power shutdown controls were not easily accessible at exit points.

Ten installations had computers in operation in areas where overhead water or steam pipes—excluding sprinkler systems—existed with inadequate provision for drainage.

Two installations had computers which were used in basements below ground level, exposing systems to potential flooding conditions.

Seven installations allowed vendor service personnel near computer banks without supervision.

Five installations allowed in-house service personnel to move about without supervision in computer areas.

Three installations located computers in quarters that were vulnerable to vandals.

Five installations managed their computers in ways susceptible to theft or misuse. Remotely located computer systems were in operation without controls to detect improper or erroneous attempts to use computers or data files.

Fourteen installations lacked contingency planning. Computerized systems were in operation without formal contingency plans to insure continuity of operations if an event occurred that threatened security.

GAO studied instances in which major data processing facilities had been hit by terrorism, vandalism, fire or natural disaster.

GAO said attempts at sabotage of computer activities have been made by employees within data processing centers. GAO said four attempts had been made to sabotage computer operations at Wright-Patterson Air Force Base near Dayton, Ohio, during a 6-month period ending November 15, 1974, by using magnets, loosening wires on the computer mainframe and gouging equipment with a sharp tool.

On August 24, 1970, a bomb exploded outside the Sterling Hall Building at the University of Wisconsin. This building housed the Army Mathematics Research Center and other federally funded research activities. One employee was killed and three others were injured. The explosion damaged 25 buildings at the university and resulted in a total loss of \$2.4 million for buildings and equipment. Computers at the Army Mathematics Research Center were damaged and some programming efforts and 20 years' accumulated data was destroyed. It has been estimated that this research data represented more than 1.3 million staff hours of effort. GAO calculated this effort to represent an investment of \$16 million.

In May of 1972, a bomb exploded on the fourth floor of the Pentagon above the computer facility and caused extensive damage. The computer facility was flooded from broken water pipes and parts of it were inoperable for about 29 hours.

The computer center at the National Institutes of Health, Bethesda, Md., has experienced many computer system failures due to electrical power failures. GAO said officials of the computer center estimated that they lost a minimum of \$500,000 annually from electrical power fluctuations. During a 15-week period, the NIH computer center experienced 6 major electrical power fluctuations which caused 15 computer system failures. These failures resulted in destruction of data for 375 batch processing jobs and for 2,250 remote terminal users. GAO said these power fluctuations caused replacement of electronics costing more than \$94,000 in various components of the computer systems.

On June 24, 1972, water from the Susquehanna River flooded all of downtown Wilkes-Barre, Pa., and filled the basement of the post office building. Water continued rising until about 6 inches of it were on the computer room floor. About \$7.5 million worth of Government computer equipment was located on raised flooring on the first floor.

Had the water risen about an inch more it would have ruined virtually all of the computer equipment, GAO said.

GAO described a 1959 fire at the Pentagon which destroyed three complete computer systems valued at \$6.5 million. The fire started in a vault containing stored paper and magnetic tape and spread throughout the computer center. When the first occurred employees were unable to reach the switch to turn off electrical power for the computer system. This created a hazardous situation for firefighting efforts.

GAO cited another example of catastrophic loss caused by fire to a Government facility, although computer records were not directly involved. In July of 1973, fire broke out in the Military Personnel Records Center in St. Louis, Mo. Sections of the building housing these records were not equipped with sprinkler systems, smoke detectors or fire walls. Although the fire did major damage to papers and not computerized records, GAO said, it nevertheless illustrated how devastating the loss of irreplaceable documents and records can be. GAO said that since such records are being put on computers more and more, the problem increasingly becomes a computer security problem.

GAO said the St. Louis records center has been the repository for about 52 million records on military personnel actions since 1912. The sixth floor, where the fire started, contained about 22 million military personnel files or jackets. About 16.8 million of these records were lost.

Of the St. Louis fire, GAO auditors said :

This installation's mission is to maintain these official government records and to respond to inquiries made by the Congress, other government agencies and the taxpayer. This mission will now be hampered for some time because the lost records—some of which may be irreplaceable—must be reconstructed to satisfy inquiries, which is a costly and time-consuming process.

While it is unreasonable to expect that there would be backup for every original record in the manual files, it is reasonable to assume that some sort of contingency planning should have been done to insure continuity of operations when a loss has occurred. Agency officials told us that a contingency plan was formulated after the fire happened.

GAO cited an instance at Kelly Air Force Base in San Antonio, Tex., in which someone altered a computer program that resulted in a \$100,000 theft of Government money. Due to the computer alteration, the Air Force paid \$100,000 to bogus companies for aircraft fuel never delivered. The bogus companies were established by a Government employee working at the base. The employee had in-depth knowledge of the computerized fuel accounting system which he helped develop and install. An investigation was begun when a bank contacted the Air Force regarding suspicious banking transactions involving Government checks. The employee was arrested, convicted and sentenced to 10 years in prison.

Among the agency comments to the GAO report were these :

James T. Lynn, Director of the Office of Management and Budget, said the GAO report was correct in citing a "need for greater awareness of threats to physical security" in automated data processing. However, Lynn said OMB did not support GAO's recommendation that an official in each agency be assigned responsibility for computer security. Instead, Lynn said, the head of each agency should decide

how computer safeguards should be provided and who should be in charge.

Terence E. McClany, Assistant Secretary of Defense, Comptroller, said of the GAO report that in general, "the importance of the subject, the general substance of the report, and the thrust of the recommendations are wholeheartedly endorsed * * *"

John D. Young, Assistant Secretary of HEW, Comptroller, said, "We fully concur with the recommendations contained in the report . . ."

William S. Heffelfinger, Assistant Secretary for Administration in the Department of Transportation, endorsed the GAO study.

The GAO report did not identify any of the specific installations where it discovered inadequate safeguards against computer damage. GAO auditors felt that to identify these sites would be to run the risk that persons might wish to exploit these security weaknesses.

Mr. President, as chairman of the Senate Committee on Government Operations, I have directed the staff to conduct a preliminary inquiry into the problems associated with computer-related crimes in Federal programs, automated decisionmaking computers in Federal programs and computer security in Federal programs.

REPORT TO THE CONGRESS BY THE COMPTROLLER
GENERAL OF THE UNITED STATES—APRIL 23, 1976

IMPROVEMENTS NEEDED IN MANAGING AUTOMATED
DECISIONMAKING BY COMPUTERS THROUGHOUT
THE FEDERAL GOVERNMENT

Computers in Federal departments and agencies annually issue unreviewed payments and other actions involving billions of dollars in Government assets. These actions are often wrong. They can cost the Government huge sums of money; exactly how much no one knows.

This report describes the ways computers issue unreviewed actions and the causes for incorrect actions. It suggests remedies to correct the situation Government-wide.



COMPTROLLER GENERAL OF THE UNITED STATES
WASHINGTON, D.C. 20548

B-115369

To the President of the Senate and the
Speaker of the House of Representatives

Many Federal agencies use computers to initiate actions that are not reviewed by people. This report describes the many problems that have been experienced by agencies that use computers this way and offers some suggestions on how to solve them.

We made our study pursuant to the Budget and Accounting Act, 1921 (31 U.S.C. 53), and the Accounting and Auditing Act of 1950 (31 U.S.C. 67).

We are sending copies of this report to the Director, Office of Management and Budget; the Secretary of Commerce; the Administrator of General Services; and the heads of Federal departments and independent agencies.

James B. Steeds
Comptroller General
of the United States

DIGEST

Federal agency computers cause more than 1.7 billion payments and other actions a year without anybody reviewing or evaluating whether they are correct. Many agencies use computers in this way. At a minimum, Government computers issue annually:

- Unreviewed authorizations for payments or checks (excluding payroll) totaling \$26 billion;
- Unreviewed bills totaling \$10 billion;
- Unreviewed requisitions, shipping orders, repair schedules, and disposal orders for material valued at \$8 billion.

COMPUTERS CAN ISSUE INCORRECT ACTIONS

Computers are complex data processing machines which are indispensable to the day-to-day operations of most Federal agencies. They can process data quickly and are especially useful in business-type applications which involve repetitive processing of large volumes of data. However, computer actions are only as good as the computer programs (or software) that make the computers operate and the data within the system. Computers can cause incorrect actions if these factors are wrong. The result is overpayments and unnecessary or premature costs.

Some agencies' internal audit reports show that unreviewed incorrect actions have been issued by several Government computers, incurring overpayments and unnecessary or premature costs of tens of millions of dollars annually. For example:

- Computers of one military department incurred increased inventory pipeline and transportation costs of \$2.2 million because of erroneous software.
- One military agency's computer caused millions of dollars in unnecessary and/or premature overhaul of equipment because of software and data problems.

Computers issuing incorrect actions over an extended period of time increase the impact of overpayments, unnecessary costs, and so on. It is important to detect incorrect actions. It is equally important to correct them as early as possible.

In this report, software that instructs computers to issue unreviewed actions are being called automated decisionmaking applications.

CAUSES FOR INCORRECT COMPUTER ACTIONS

Incorrect computer actions occur because of software problems and/or data problems. The causes of these problems are numerous.

Software problems, for example, can be caused by inadequate communications between people involved in software development.

Data problems, for example, can be caused by the use of input forms that are too complex.

FEDERAL POLICY AND AGENCY MANAGEMENT

There is no Federal-wide policy, guidance, or other instructions on how computers issuing unreviewed actions should be managed by Fed-

eral agencies. There is little checking or monitoring of output on an ongoing or short-term periodic basis. Internal audit reviews of these computer actions are made sporadically or not at all.

Several things can be done that will disclose some of the problems before they occur and/or before computers make decisions that can cause incorrect actions for an extended period. These practices should be considered for Government-wide use.

RECOMMENDATIONS

GAO believes that, since automated decisionmaking applications have not previously been recognized as a separate problem area requiring management attention and since millions of dollars are presently being wasted as the result of actions generated by such systems, the Office of Management and Budget should act immediately to improve the situation. Specifically, GAO recommends that the Director, Office of Management and Budget, in his oversight capacity, require that:

- Each agency determine whether any of its computer operations involve automated decisionmaking applications.
- The agencies review each operation to determine whether incorrect actions are being taken as a result of these applications. (Pending issuance of technical guidelines by the National Bureau of Standards for making such reviews, the agencies should examine enough automatically generated decisions to provide a basis for deciding whether incorrect decisions are occurring and, if so, should take the necessary steps to correct the situation causing the inaccurate decisions.)
- Before any new automated decisionmaking applications are initiated by an agency, the proper steps are taken to insure correct decisions. This would include, pending issuance of National Bureau of Standards guidelines, a carefully chosen combination of independent review of systems design, adequate testing before implementation, and periodic testing of decisions after implementation, as discussed in this report.
- Agencies make reports on the actions taken, and establish an appropriate mechanism for monitoring reports.

GAO recommends that, because the National Bureau of Standards has responsibilities for technical aspects of automatic data processing, the Secretary of Commerce direct the Bureau to issue technical guidelines for developing, using, technically evaluating, documenting, and modifying these applications in the Federal Government. When issued, these guidelines should contain certain criteria for independent technical reviews and for monitoring of these applications to insure problems are detected and corrected promptly. The general Services Administration should incorporate the Bureau guidelines in its agency directives.

In addition, GAO recommends that:

- As the General Services Administration suggested, the Civil Service Commission develop and add to its automated data processing training curriculum courses in automated decisionmaking applications so that managers, technical personnel, and auditors will

become better equipped to deal with them in an appropriate manner.

—Internal audit groups in agencies having automated decisionmaking applications participate actively in design, test, and reviews of such systems to carry out their responsibilities.

Finally, GAO suggests that the Joint Financial Management Improvement Program consider this area for ongoing attention.

GAO is sending copies of this report to all departments and independent agencies for their information, use, and guidance pending issuance of the Office of Management and Budget and the National Bureau of Standards material.

GAO received comments from several agencies. They agreed in principle to the need for increased management attention to automated decisionmaking applications.

CHAPTER 1

INTRODUCTION

Many early business applications on computers involved entering, manipulating, and summarizing data and generating reports. Most output produced by these computers was manually reviewed (1) for correctness and/or (2) to decide what actions should be taken on the basis of the output report.

As more complex computer processing developed, the applications became more innovative. Computers were assigned certain repetitive decisionmaking work which duplicated steps people had taken to do the job previously. The output of these computers is frequently not reviewed by people (that is, no manual review).

These types of applications have no established name. We are calling them automated decisionmaking applications.

AUTOMATED DECISIONMAKING APPLICATIONS

Automated decisionmaking applications are computer programs that initiate action (through output) on the basis of programmable decisionmaking criteria established by management and incorporated in computer instruction. The distinguishing characteristic of these applications, as compared to other computer application programs, is that many of the computer's actions take place without manual review and evaluation.

An inventory application is an example of a computer application program. If the computer processing of a requisition for material reduces the onhand quantity below the reorder point and if the computer issues a purchase order without anyone reviewing the proposed procurement quantity, then the application is an automated decisionmaking application. Some of the computer output of these applications is reviewed. In the foregoing example, the application may call for manual reviews of quantities on all purchase orders over \$5,000, with all purchase orders under that amount being released without review.

We reviewed these applications because (1) billions of dollars are involved in the unreviewed actions that they initiate and (2) of indications that funds were being wasted because of incorrect actions.

CHARACTERISTICS

One objective of using computers operating under automated decisionmaking applications is to take advantage of their speed, accuracy, storage capabilities, and capacity to obey predetermined instructions. These applications are needed in part, because of the tremendous volumes of information to be obtained, manipulated (processed), analyzed, and acted on in carrying out agency missions and goals.

Automated decisionmaking applications process large volumes of transactions put into the computer system from various sources. They make repetitive decisions that, in many cases, previously have been made by people. The decision instructions, built into the program, ask questions about the transactions and then initiate many actions through output. The actions depend solely on the criteria (logic) and data inside the computer system.

Computer program

The computer program (software), written by people, instructs the computer (1) to examine the input data and/or data already in automatic data processing (ADP) files, (2) to perform logical decisionmaking steps and computations in processing the data, and (3) to initiate actions in the form of output as a result of this process.

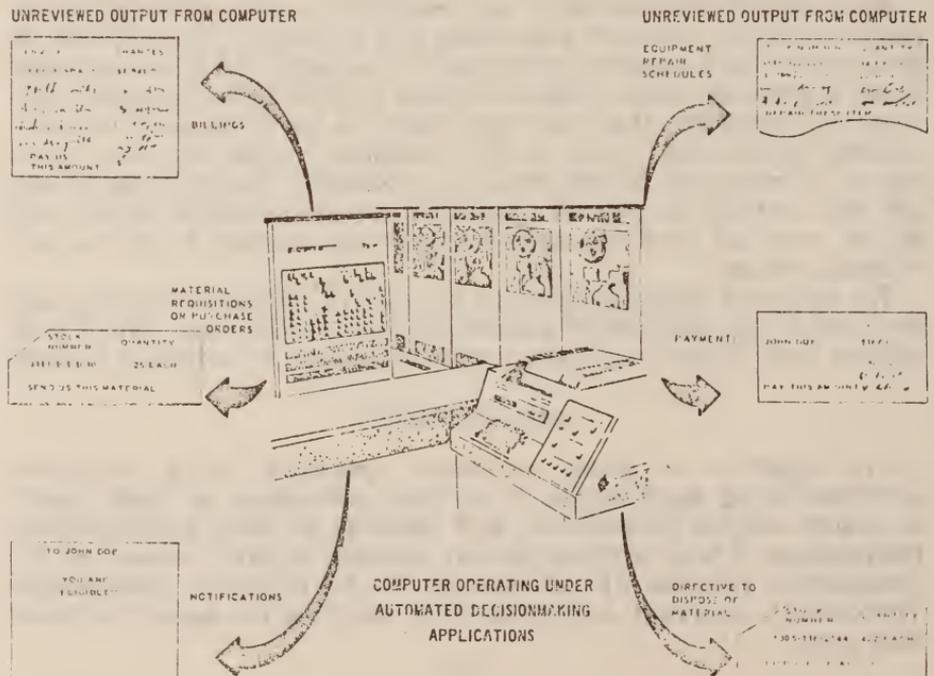
Input

Data is usually obtained by people from various sources and is put into the computer in machine-readable form (including punched cards, optical character recognition documents, paper tape, magnetic ink character recognition documents, and direct keyboard entry). The data can be entered directly for processing or can be recorded on ADP files for processing at a later time.

Output

The application outputs are such things as (1) directives to act (such as orders to ship material), (2) payment authorizations or checks, (3) bills, and (4) notices. A large percentage of the output of these applications is not manually reviewed and evaluated by people.

The following illustration shows a computer operating under automated decisionmaking applications.



The form of output varies (including listings, magnetic tapes, pre-printed forms, and punched cards). These outputs indicate the decisions resulting from computer processing directed by the software.

The outputs that are not reviewed or evaluated are usually issued to the organizations and people which take the action being directed or which are being paid, billed, or notified.

Some of the output of many automated decisionmaking applications is manually reviewed. Under "management by exception" principles, some output, the nature and extent of which is determined by management, is sent to people in the organization for manual review and evaluation. This technique allows people to consider criteria, factors, and information not contained in the computer system in deciding whether the computer-directed action should be taken. For these applications manual intervention takes place only for the actions output for review.

The criteria for directing manual review of the output are contained in the decisionmaking part of the program. In the inventory application example, the program would direct that purchases over \$5,000 be output for manual review. The applications can be programmed so that none of the output will be manually reviewed or evaluated before actions are taken.

CONTRAST WITH OTHER COMPUTER APPLICATIONS

Application programs designed to provide output to people for information and analysis are not automated decisionmaking applications. Many types of these application programs are used in Government, and the outputs are sent to people for review before actions are taken.

Typical application programs that are *not* automated decision-making applications include:

- Systems that make recommendations, all of which are manually reviewed before actions are taken;
- Management and other information systems which provide data to various levels of managers to assist them in making policy, management, and operating decisions;
- Most mathematical models.

CHAPTER 2

USE OF AUTOMATED DECISIONMAKING APPLICATIONS BY FEDERAL AGENCIES

Many Federal agencies use automated decisionmaking applications to support their functions. Annually, more than a billion actions, involving billions of dollars, in directives to act, to make payments, to issue orders for material, and to bill for amounts owed are initiated. They also issue millions of notifications to people outside the Government.

INFORMATION ABOUT AUTOMATED DECISIONMAKING APPLICATIONS USED BY FEDERAL AGENCIES

We wanted to learn how these applications were used and to obtain data on their characteristics and monetary impact on Federal operations, but we found no central inventory. We therefore developed a questionnaire to gather information about Federal automated decisionmaking applications and distributed it to 15 agencies that use computers extensively. The information we wanted included:

- Functions supported by these applications;
- Numbers of these applications and their impact on operations (including output produced and annual volume and monetary impact);
- Whether certain parts of the decisions were being manually reviewed.

We obtained more detailed information about selected automated decision making applications to understand and illustrate typical uses.

Almost all the agencies we contacted gave us examples of their automated decisionmaking applications. The information is summarized below.

	<i>Number of examples times function was cited</i>
Defense departments and agencies :	
Air Force	14
Army	14
Defense Supply Agency	9
Navy	18
Total	55

Civil departments and agencies :	
Agriculture	6
Commerce	4
General Services Administration	5
Health, Education, and Welfare	8
Housing and Urban Development	6
Interior	10
Transportation	18
Treasury	4
Railroad Retirement Board	3
Veterans Administration	9
Total	73

Total number of examples obtained—128.

FUNCTIONS SUPPORTED BY AUTOMATED DECISIONMAKING APPLICATIONS

The questionnaires showed that automated decisionmaking applications supported many functions. A compilation of responses is presented below :

Function :	<i>Number of examples</i>
Controlling	48
Notification	48
Fiscal	46
Payment	46
Supply	44
Billing	41
Distribution	38
Eligibility	31
Maintenance	30
Procurement	30
Diagnostic	23
Scheduling	20
Disposal	17
Cataloging	13
Personnel	11
Safety	9

NUMBER OF AUTOMATED DECISIONMAKING APPLICATIONS AND THEIR IMPACT ON FEDERAL AGENCIES

No one collects statistics on these applications for the Federal Government as a whole, so we could not determine the total number. Some of the agencies responding to our questionnaire said their responses consisted of representative applications. Therefore, our report about automated decisionmaking applications and their impact represents only a part of the Federal-wide total.

The responses identified 128 applications which issued several different types of unreviewed output. The nature of the output and its estimated annual impact on Federal operations, both in volumes and dollars, are summarized below.

Nature of output	Number cited	Total actions (thousands)	Total monetary impac (millions)
Payment authorizations or checks to:			
Contractors or grantees.....	10	8,700	\$7,221
Members of the public.....	23	715,000	18,589
Government employees (other than payroll).....	3	200	8
Bills sent to:			
Contractors.....	3	100	15
Government organizations.....	17	17,300	6,549
Members of the public.....	18	19,100	3,298
Purchase orders or supply requisitions.....	24	28,000	4,456
Directives to ship material.....	22	260,200	12,500
Directives to dispose of material.....	11	8,000	156
Production, repair, or rework schedules or instructions.....	12	191,300	1,150
Notifications to members of the public.....	21	22,200	NA
Other.....	48	447,300	NA
Total.....	212	1,717,400	

¹ Represents the value of material on which these actions were taken. Information collected indicates that the transportation costs represent about 5 percent of the value of material shipped; the disposal costs about 3 percent of the material disposed of; and production, repair, or rework cost about 23 percent of the value of the material.

Note: The actions and monetary impact in the preceding schedule are for only a portion of the 212 output types. Many responses indicated that this data was not readily available. Our followup confirmed this.

REASONS FOR OUTPUT OF ACTIONS FOR MANUAL REVIEW AND EVALUATION

Some of the applications initiate all actions without review. Most are designed, however, under the management-by-exception principle, which results in some of the output being reviewed by employees before the actions are implemented.

Several reasons given by agencies for reviewing some of the output are shown below.

	<i>Times cited</i>
Monetary value of indicated action exceeds prescribed dollar limitations.....	43
Criticality of the action to be taken.....	28
Eligibility factors related to the action.....	21
Geographic considerations of various types.....	11
Health and safety considerations related to the action.....	10

The percentage of actions initiated automatically varies from one application to another and can be adjusted by changing the processing criteria. The percentage of unreviewed actions identified by agencies participating in this study is shown below.

Percent of action unreviewed :	<i>Number of applications</i>
100.....	15
90 to 99.....	42
80 to 89.....	13
70 to 79.....	14
60 to 69.....	5
50 to 59.....	3
Below 50.....	14
No data provided.....	2
Total.....	128

AN EXAMPLE OF WHAT AUTOMATED DECISIONMAKING APPLICATIONS DO

Automated decisionmaking applications are designed to make internal decisions of varying degrees of complexity and to generate output containing the action to be taken. An example of one of these applications is shown in this section. Other examples are presented in chapter 3.

Customer returns program

The Defense Supply Agency (DSA) uses an automated decision-making application—credit returns—to evaluate inquiries from military activities on what to do with surplus DSA-managed material. The options are to (1) return the material for credit, (2) return it without credit, or (3) dispose of it.

DSA's computers receive the requests in machine-readable form. The application identifies the commodity and refers to pertinent data about it from the ADP files (such as information on the quantities of the material already stored in DSA's inventory and expected future requirements). Using this and still other data, the application tells the activity what to do with the material. Usually these directives are sent without manual review.

During a recent 1-year period, two of the six DSA supply centers issued the following unreviewed directives using this application.

Nature of directives	Estimated volumes of unreviewed directives issued	
	Directives	Value of material
Ship the material (with or without credit) to the DSA supply system.....	174,000	\$76,000,000
Dispose of the material.....	62,000	24,000,000
Total, unreviewed advices.....	236,000	100,000,000

CHAPTER 3

AUTOMATED DECISIONMAKING APPLICATIONS CAN MAKE BAD DECISIONS

Whether actions initiated automatically by the computer are correct or not largely depends on (1) the internal logic of the program and (2) the data that is fed into the system.

Computers will produce bad decisions (1) if programmers and analysts make misjudgments or errors in establishing the decision-making criteria or (2) if the application is not designed and/or coded in a manner that properly implements the decisionmaking criteria. Changing circumstances can make adequate decisionmaking criteria in the software obsolete, and bad decisions will occur if the software is not changed. Failure to design appropriate checks on input data, such as edit checks, can contribute to bad decisions. These applications can also make bad decisions if the data supplied to them is incomplete or incorrect or if the data is not obtained or processed quickly.

Some internal audit groups have reported on bad decisions made by Government automated decisionmaking applications. The computer-initiated actions caused the agencies to incur tens of millions of dollars of unnecessary costs, premature costs, and overpayments.

Such bad decisions may also harm individuals and impair an agency's ability to carry out its mission effectively.

CONDITIONS LEADING TO BAD DECISIONS

Adverse conditions common to several agencies have been reported. These conditions, resulting in the applications automatically initiating uneconomical or otherwise incorrect actions, can be broadly categorized as (1) software problems and (2) data problems.

Software problems

Several software problems that can cause bad decisions by automated decisionmaking applications include:

- Designing software with incomplete or erroneous decisionmaking criteria. Actions have been incorrect because the decisionmaking logic omitted factors which should have been included. In other cases decisionmaking criteria included in the software were inappropriate, either at the time of design or later, because of changed circumstances.
- Failing to program the software as intended by the customer (user) or designer, resulting in logic errors often referred to as programming errors.
- Omitting needed edit checks for determining completeness of input data. Critical data elements have been left blank on many input documents, and because no checks were included, the applications processed the transaction with incomplete data.

Data problems

Input data quality is frequently a problem. Since much of this data is an integral part of the decisionmaking process, its poor quality can adversely affect the computer-directed actions. Problems include:

- Incomplete data used by automated decisionmaking applications. Some input documents prepared by people omitted entries in data elements which were critical to the application but which were processed anyway. The documents were not rejected when incomplete data was being used. In other instances data which the application needed and which should have become part of ADP files was not put into the system.
- Incorrect data used in automated decisionmaking application processing. People have often unintentionally introduced incorrect data into the ADP system. This incorrect data affected application decisions.
- Obsolete data used in automated decisionmaking application processing. Data in the ADP files became obsolete due to new circumstances. The new data may have been available but was not put into the computer.

Conditions that have been reported by internal audit

Unfavorable conditions were identified by 32 internal audit reports of 7 agencies. These reports, issued during a 23-month period, demonstrated that the same conditions occurred in different agencies and were therefore common problems. The audit reports, however, did not show the total occurrences and dollar impact of these conditions, past or present, in federal automated decisionmaking applications.

The results of our analysis of these audit reports are summarized in the following table. (For further details, see app. V.)

Category and condition	Agencies	Internal audit reports	Times condition was reported ¹
Software problems:			
Incomplete, erroneous or obsolete decisionmaking criteria.....	7	14	30
Programming errors.....	5	10	10
Criteria or programming ²	5	11	14
Absence of needed edit checks.....	4	5	11
Data problems:			
Data elements incomplete.....	6	10	16
Data elements incorrect.....	5	17	30
Data elements obsolete.....	3	3	3

¹ Each condition can occur more than once. Software problems, such as programming errors, may have occurred in more than 1 portion of the program or the condition may have been observed at more than 1 location, each designing its own program. The data conditions were based on the number of different data elements that were either incomplete, incorrect, or obsolete at least once.

² Internal audit reports were not sufficiently detailed to arrive at an opinion as to whether the problem was in criteria or programming.

Only 13 of the 32 reports had estimates of the monetary impact of bad decisions, but these estimates ran to tens of millions a year in unnecessary and premature costs and in potential overpayments. Some reports cited specific cases but provided no estimates of the total monetary impact. Other reports cited potential mission impairment and possible harm to individuals.

The following sections are based on internal audit reports selected from the 32 reports obtained.

SOFTWARE PROBLEMS REPORTED

Examples of software problems are presented to demonstrate the problems frequently experienced with automated decisionmaking. The examples are not intended to be a criticism of the agencies involved, because these problems can occur wherever these applications are used.

Army processing of requisitions for shipment to overseas locations

Several Army inventory control points provide material support to overseas customers which submit requisitions for materials to the control points. Automated decisionmaking applications are used to screen material availability at U.S. depots. The computer produces a directive which is automatically issued to a depot to ship material to the overseas customer. These applications process over 100,000 overseas requisitions annually.

Early in the 1970s the Army implemented a system designed to improve supply support to overseas customers from U.S. depots. The control points were instructed to design their ADP applications so that material would be issued from east coast depots to satisfy European customers and from west coast depots to satisfy Pacific customers. Controls were required to prevent the software from releasing cross-country shipments without manual review.

The Army Audit Agency examined the applications in effect at five control points. At four activities it found that the applications were not adequate to insure maximum filling of requisitions from the appropriate depots. For instance, in the initial requisition processing for overseas customers, the software used by one of the high-volume control points screened stock availability at eight depots before finding the appropriate depot. For releasing back-ordered-stock requisitions, depots on the opposite coast were often selected for material availability. The auditors reported that, at three control points, controls to prevent the automatic release of material from the wrong depots were not implemented and material was automatically released for cross-country shipments. At least two control points used software that existed before the criteria for supporting overseas activities were developed.

The audit agency estimated that, because of the use of this erroneous criteria, unnecessary transportation costs of \$900,000 a year were incurred. In addition, \$1.3 million was incurred in increased inventory investment (pipeline) costs.

The Army Materiel Command agreed with the audit agency's assessment of the problem and promised to revise the criteria contained in Army control point applications.

Navy scheduling of aircraft equipment for overhaul

The Navy's central manager for aircraft spare equipment and parts uses a computer to identify and schedule overhaul for reparable components needed for future use. Until April 1974 the application used was called the Navy integrated comprehensive reparable item scheduling program.¹

¹ In April 1974 the Navy integrated comprehensive reparable item scheduling program was replaced by another automated decisionmaking application called cyclical repair management. We believe that the problems that occurred in the first program could affect cyclical repair management in a similar way, but GAO's review did not evaluate the new program.

This application considered inventory on hand, requirements, and other data in ADP files to determine

- Which components should be scheduled for overhaul;
- What quantities should be overhauled;
- Which depots should do the work; and
- What priorities depots should give in deciding which items should be overhauled first.

Depots used punched card output as the basis for scheduling components for induction into their overhaul facilities. Priority levels shown on the output affected the depots' decisions regarding which items and quantities would be overhauled first. (Not all the quantities the program indicated for overhaul were processed because of limited depot overhaul capacity.)

The priority levels shown in the output ranged from level 0 (zero)—highest priority—to level 3—lowest priority.

During a 1-year period,² Navy facilities spent about \$145 million to overhaul aircraft components valued at about \$797 million—mostly on the basis of the program's output. The Naval Audit Service, reviewing the operation, identified several major software problems, all of which resulted in overstating overhaul requirements.

- A data element used in computing priority level 1 contained data that resulted in duplications in computing levels 2 and 3. Gross overhaul requirements scheduled by the program were therefore overstated. When the program was designed, this duplication was overlooked.
- Data elements showing recurring material usage, used to compute levels 2 and 3, were greatly overstated because of two software problems.

1. Required reductions to the material usage quantities were not made automatically, because certain Navy activities were leaving a data element blank on input documents sent to the central manager. Our followup determined that because of the designer's oversight or judgment error, no edit check was placed in the software to detect this missing data.

2. There were no software procedures for automatically reducing recorded material usage quantities when customers canceled back orders and requisitions. Our followup disclosed that when this application was designed, the designer believed that canceled back orders and requisitions would rarely occur.

The Naval Audit Service estimated the effect of these incorrect actions was millions of dollars in unnecessary and premature overhaul costs. Although the Navy Command officials did not agree with the auditor's reported figures, they agreed that the problems identified were valid. Corrective actions have been taken or initiated.

A GAO report (B-162152, May 21, 1974) "Better Methods Needed for Canceling Orders for Materiel No Longer Required" discussed the Navy's practice of not automatically reducing recorded material usage when unfilled customer orders were canceled. The report stated that "we estimate that this overstatement resulted in annual unnece-

² The figures presented are for an overlapping but not identical period. The overlap is 6 months.

sary materiel buys and repairs totaling about \$10 million." Of that amount, more than \$3 million was for repairs initiated by this automated decisionmaking application.

DATA PROBLEMS REPORTED

The following examples of data problems show how bad data can adversely affect the actions directed by automated decisionmaking applications.

Veterans Administration payments for apprenticeship and other on-job training

The Veterans Administration (VA) uses a computer application to make monthly payments to more than 185,000 veterans in apprenticeship or other on-job training. This application is designed to make payments at a rate that decreases every 6 months, under the assumption that veteran's pay will increase as he learns his trade.

Data put into the computer is the basis for automatically determining the rates at which the veteran will be paid. Each month, additional data is put in regarding the veteran's continuing eligibility to receive the payments.

This application is programed to read input documents and distinguish apprenticeship and other on-job training awards from other types of education awards. When the application recognizes these on-job training awards, it refers to appropriate rate tables to determine the proper payment. The application refers to a new lower rate every 6 months and automatically initiates payments at the reduced rate. Annually, this application initiates about 1.4 million unreviewed checks for more than \$225 million in apprenticeship and other on-job training awards.

Two types of input documents initiate payments for these awards. An original award document is designed to initiate payments to a veteran not previously receiving them. If the veteran has already received benefits and there is a need for (1) reentrance, (2) a supplemental award, or (3) new key data such as dependency changes, a different input document (supplemental award code sheet) is prepared. Both documents contain data elements that allow the computer to determine that it is an apprenticeship and other on-job training award and that the reducing rate table should be used.

The data entry on the supplemental award document that causes the program to build the scheduled rate reduction is code 77 in a data element called change reason.

VA internal auditors reported that 22 of 121 tested supplemental award documents for these benefits did not contain change reason code 77 on the input documents (the data problem). These documents were received from 10 different VA locations. The application accepted and processed the documents because the software did not contain an edit check to disclose and reject documents with incomplete entries in this data element (a related software problem).

Because the data was incomplete, the computer used a single rate for the entire period of training at the highest step indicated. This problem caused potential overpayments of \$700,000.

Possible causes cited for processing incomplete input documents included new personnel—requiring additional training—and fatigue. The designer overlooked the needed edit check, a software problem, in preparing the detailed and complex software.

Army processing requisitions for radioactive material

The Army uses a computer to automatically process customer requisitions for commodities. One Army agency uses an application to process at least 250,000 requisitions annually for material valued at a minimum of \$250 million. About 35 percent of the customer requisitions are output for manual review and evaluation for any of several reasons. The remaining 65 percent are processed without manual review.

Some commodities the agency manages contain radioactive material. The Army master data ADP file is supposed to contain a special control code (code 8) in a specific data element for commodities containing radioactive material. This code, which should be put in by item managers, prevents automatic issues. The item managers receive commodity requisitions for review and evaluation. This manual intervention is required to insure that the requisitioners are (1) authorized to receive the material, (2) aware of the radioactive content, and (3) aware of the safeguards that must be used.

The Army Audit Agency reviewed 86 radioactive commodities which the agency managed to determine if the proper special control item codes were contained in ADP files. The review showed that 29 of the commodities were incorrectly coded.

—Eleven commodities were coded as a regulated item (code 1) but not as radioactive. (A regulated item is one that is scarce, costly, or highly technical.)

—Eighteen commodities contained an 0 code in the ADP files. An 0 code indicates that no special controls or handling are required. Many requisitions for these commodities are processed automatically.

Most of the incorrectly coded commodities had been in the supply system 4 to 13 years.

During the Audit Agency's review of 1 year's transactions, at least 38 customer requisitions were automatically filled for 18 incorrectly coded commodities. Army customers and foreign governments under military assistance programs were issued 423 units on these 38 requisitions.

Since the commodities were incorrectly coded, the item managers did not coordinate the issue of the units with the 38 customers. Consequently, there was doubt that the customers should have been issued the material or that they were aware of the radioactivity in the commodities.

Army officials cited the following possible reasons for the incorrect codes contained in ADP files.

—The item managers who prepared the input to ADP files may not have been fully aware of the requirements and procedures for coding radioactive material.

—The agency's health physicist may not have notified the item managers of the radioactivity contained in these commodities.

—The item managers may have been notified but failed to input the correct data codes.

Army officials agreed with the Audit Agency's findings and said they would (1) correct the ADP files for all radioactive commodities, (2) reemphasize to item managers the need for assigning the proper special control item code to commodities, and (3) have a health physicist study the commodities to insure that the items could be used safely by the customers that received them automatically. The special study determined that the commodities involved could be safely used by the recipients.

INTERNAL AUDITS OF AUTOMATED DECISIONMAKING APPLICATIONS

Since published internal audit reports were the sources of our information on bad decisions, we asked nine internal audit groups about the nature, approaches, and frequency of scheduling audits of these applications.

We learned that certain internal audit groups rarely became involved in the applications' logic because they lacked the expertise to effectively make such studies.

No internal audit group has prepared lists of agency automated decisionmaking applications and scheduled reviews of their decisions, either routinely or when the system is modified. However, several audit groups schedule specific agency functions for audit, and if the functions are supported by these applications, auditors will get involved in the internal decisionmaking logic to evaluate the agency's performance.

Agency functions are generally audited on a cyclical basis, but the cycle may be anywhere from 2 to 8 years. Ordinarily, the frequency of review is not dependent on whether the function is supported by an automated decisionmaking application. In addition, auditors may review functions and related automated decisionmaking if there is (1) a special request or (2) an indication of a problem based on complaints. On the basis of approaches taken by internal audit groups, it appears that many of these applications go unaudited for long periods of time or may never be audited.

Although many of the audit reports adequately show many of the common problems that exist, they do not show the overall impact of the problems for all automated decisionmaking applications. In fact, there is no basis for estimating the total impact of bad decisions currently being made by these applications.

CHAPTER 4

CAUSES OF BAD AUTOMATED DECISIONS

The two basic automated decisionmaking application problems, software and data, are often interdependent. For example, automated decisionmaking applications making bad decisions because of incomplete data elements on input documents illustrate both a data problem and a software problem because (1) input documents have not been properly prepared (data) and (2) edit checks for completeness have not been properly designed (software). Other problems, such as when incomplete or erroneous decisionmaking criteria are used (software) and incorrect data is put into the application (data), can occur independently.

The problems in each of these two areas are caused by a variety of factors. We identified many causes of these problems by (1) corresponding with people experienced in software design and data management, (2) discussing them with officials of selected Federal agencies, and (3) analyzing published internal audit reports.

SOFTWARE PROBLEMS

Computer programs are usually developed and modified by a combination of people; the user (or customer), that requires the computer assistance; the designer (or analyst), who translates the requirements of the user into a logical structure; and the programmer, who translates the logic into program instructions which can be recognized and used by the computer.

The software development and modification process was similar at each Federal agency we visited. Variations are not related to the process itself but rather involve such factors as

- organizational setup and physical locations;
- titles of people performing various aspects of the work; and
- nature of the documentation that will be prepared, such as use of program flow charts.

Causes of software problems

Agency officials said that the design or modification and programming of software could not be guided by specific instructions on how best to do the work. Instead, agencies rely on people who know (1) the function supported by the computer and (2) the art of design and coding so that the computer can perform the desired tasks. Some agencies provide broad guidelines on the process, the documents to be used in the process (documentation), and at one agency, instructions on what designers and programmers should consider when doing the work.

The user initiating the work sets forth many of the specifics regarding the internal decisionmaking criteria to be used. Often the designer makes some decisions. Both act on the basis of their knowledge of the function, available guidelines in terms of management instruction or legislation, their perceptions of the transactions to be processed, and communications with each other. Sometimes they will call on operations research experts to help them design new criteria, while sometimes they will use existing criteria to process similar transactions.

The designer takes the established criteria and prepares more specific documentation which is used for programing. The design and programing documents developed become very detailed and complex, because the computer is instructed to operate in a logical step-by-step manner on a large number of different conditions. Even less complex applications can consist of thousands of individual instructions that must be designed and programed to do what the user and designer perceive to be correct.

The designer and user are usually responsible for designing edit checks into the program. This includes checks for the completeness of data elements on input documents. According to agency officials, edit checks are placed in the software for data that is critical to the decisionmaking, such as when incomplete or erroneous data can affect the determinations made by the computer. Some officials said that edit checks are placed for almost every data element. One agency is making an overt effort to limit edit checks to reduce the number of documents rejected by the computer.

In developing software, it is generally accepted that the lines of communication between the user and designer and the designer and programer must be effective.

To identify some of the causes for the software problems presented in chapter 3, we

- Discussed them with Federal officials at several agencies;
- Received responses to questionnaires from 257 individuals who are experienced in the areas of ADP software design, modification, and programing; and
- Analyzed causes cited by internal auditors.

A schedule summarizing some of the causes of software problems is followed by a discussion of each.

Summary of Causes of Software Problems

Cause	Opinions of people answering the questionnaire-- degree of cause (note a)		Identified from contacts with officials of Federal agencies (note b)	Cited as a cause by internal auditors
	Moderate to very large	Somewhat small or none		
Inadequate communications between the parties to software design	251	4	x	
Incorrect perceptions of the nature of actual transactions to be processed	233	22	x	x
Inadequate documentation preventing adequate reviews of software	229	28	x	x
Time constraints hampering the effectiveness of the design process	216	40	x	
Absence of written criteria or guidelines for designers to follow	204	49	x	
Detail and complexity involved in designing, coding, and reviewing software	177	79	x	x
Reliance on the expertise and experience of people doing the work (state of the art)	171	83	x	x
Undetected changes in circumstances making the application obsolete	167	90	x	x
State of the art in software testing which prevents testing all possible conditions	164	91	x	

a/The questionnaire presented "some possible causes of the design conditions (problems) * * *," and asked that "based on your software design experience * * * indicate the degree to which you believe each of these causes contributes to the design condition (problems) in general." The responses allowed were to a: very large degree, somewhat large degree, moderate degree, somewhat small degree, very small degree, or not at all.

b/Our contacts were made with various organizational elements, excluding internal audit, within five agencies: Department of the Navy; Department of the Air Force; Department of Health, Education, and Welfare; Veterans Administration; and National Bureau of Standards.

The problems identified are caused at various phases of the software design process including

- User determinations;
- Designer actions; and
- Program coding.

Many problems are not detected through the review and test phases of the process and are therefore continued through implementation and operation of the automated decisionmaking application. Officials at the National Bureau of Standards and the Air Force believe that it is impossible to insure the design of completely error-free software under the current state of the art.

Inadequate communication between the parties to software design

At least three groups of people must adequately communicate to develop or modify the applications successfully. Assuming that the user knows what he wants the computer to do and that his criteria are correct, inadequate communications of this information can result in developing software that is not exactly what the user wants.

Much has been written about the communication problem in software development, and it is generally recognized as a human problem.

Incorrect perceptions of the nature of actual transactions to be processed

Decisionmaking criteria used in these applications have sometimes been erroneous, because people developing them made wrong assumptions about the nature of the transactions that were to be processed. They may have relied on limited data about the transactions and established the criteria on their judgment.

Officials of one agency believed that a large percentage of automated decisionmaking application software problems were caused at the very beginning of the design process by people involved in defining requirements and establishing decisionmaking criteria.

In other cases, the designer may have used criteria contained in existing software to process transactions in a similar, but not identical, environment. Sometimes this is done to shorten design and programing time, but it can and has caused problems.

Inadequate documentation preventing adequate reviews of software

In our October 8, 1974, report (B-115369) "Improvement Needed in Documenting Computer Systems," we noted that some agencies had not developed adequate guidelines for preparing good documentation. Several Federal officials said that this was still a problem and that documentation for many computer applications (including automated decisionmaking) was inadequate.

The report stated :

In one case documentation explaining the objectives of the computer system was not prepared by the systems analyst. Without this information, management could not adequately monitor the system's development. * * * the system did not accomplish the results originally intended by management.

In another case, inadequate documentation was cited as causing management to spend over a year to determine how the various programs in a complex system operated.

Adequate design documentation is needed to allow for

- Reviewing the work done during application design and modification;
- Making the necessary modification;
- Correcting errors when they are detected; and
- Insuring the application is operating as intended.

Time constraints hampering the effectiveness of the design process

Many systems containing these applications are designed or modified because of legislation or other high-priority requirements imposed by top management. Often this calls for implementation by a specific date. Developing and/or modifying software within the required time frames can hamper efforts to insure its adequacy. Agencies that must

make changes to these applications on the basis of legislation include VA and the Department of Health, done to shorten design and programming time, but it can and has caused problems.

Absence of written criteria or guidelines for designers to follow

Federal officials had many opinions about the need for and nature of written guidelines that should be provided to designers of software. The agencies we visited had varying degrees of formal guidelines, but none provided instructions on how to do design work.

Some officials who believe that written criteria and guidelines on how to design software are not desirable refer to the process as an art that cannot be guided or improved by written instructions. However, the consensus of responses to our questionnaires indicates that the absence of criteria or guidelines can be a major cause for some automated decisionmaking application problems.

Detail and complexity involved in designing, coding, and reviewing software

Even smaller applications can be extremely complex and detailed when designing and coding the processing logic and edit checks. The complexities and detail involved may also hamper the review process that may exist.

An illustration of the problem is VA's automated decisionmaking application for supplemental education benefit awards—which is a small part of VA's total education applications. This program consists of more than 1,100 lines of code covering about 420 decision points. One Navy automated disposal application—also a relatively minor program compared to others—contains about 7,300 lines of code with more than 290 decision points. More complex software, such as the Navy cyclical repair management program, has more than 64,800 lines of code with at least 630 decision points.

The sheer detail and complexity of the process can cause design and programming errors and omissions which are not caught in review and testing. Therefore, bad decisions occur.

Reliance on the expertise and experience of people doing the work

The nature of the design process causes agencies to rely on designers who must be experienced in both the software design and the function to be supported by these applications.

Federal designers are

- Schooled in the art of software design and learn the function to be supported;
- Experienced in an operating function and learn the art of software design; or
- Former programmers and are promoted to the design function.

Programmers are generally schooled in writing code in specific computer languages.

Much reliance is placed on the individual designer's ability to convert user requirements to the type of detailed logic needed for programmer coding. Reliance is also placed on the programmer's ability to write code according to the logic given him. Because of the detail and complexity involved, it is difficult for management to review and assess every aspect of the designers' and programmers' work.

Undetected changes in circumstances making the application obsolete

A cause for erroneous decisionmaking criteria includes the failure to identify and/or to relate changes in processing circumstances to the operation of the application. Once the application is operational, it will make decisions—good or bad—on the same basis until it is modified.

Not recognizing changed circumstances so that applications could be modified could result in bad decisions based on criteria that were correct when designed, but which no longer applied.

State of the art of program testing which prevents testing all possible conditions

The current state of the art makes it difficult for agencies to test for all conditions that may occur during the transaction processing. Most agencies cannot even be sure that the tests have exercised every line of code. As result, accepted software can contain design and/or coding errors not identified during the test phase. Some of these errors may not be detected until long after the application becomes operational.

The inability to test for all conditions also precludes a full evaluation of user and designer criteria built into the program (if and when such evaluation is attempted.)

DATA PROBLEMS

Data used by the computer in making decisions comes from a variety of sources, both internal and external to the agency that has the computer. A tabulation of the various sources of data input for the 128 automated decisionmaking applications identified is presented below.

Source of input document:	Number of applications in which the originator was cited
People within the agency operating the application-----	49
People located outside the agency operating the application but within the same Federal department or independent agency-----	23
People located in non-Government activities-----	12
People located in other Federal departments or independent agencies -----	7

Control over the completeness, accuracy, and currency of data largely depends on the source. Obviously, the correctness of an application operated at an agency where all the data comes from outside sources largely depends on the quality of data submitted. Some controls can be applied to incoming input, but they cannot guarantee completely error-free data.

According to some Federal officials, the largest single data problem is validating input data. However, data quality must be controlled from the moment data enters the system until the automatic processing is complete.

Types of controls for data

There are two basic types of controls for insuring the completeness, accuracy, and currency of data used by a computer in making decisions.

1. External controls are procedures developed outside the computer system. The objective is to check the quality of data to be put into and contained in the computer system. The controls include such things as manual procedures designed to determine if data is recorded completely and accurately on input documents and whether documents are being received and/or processed on time.

2. Internal controls generally do not involve human intervention. Many of these controls are built into the software. They include edit checks for completeness, logical relationship tests (does the data make sense?) and reasonableness checks (to isolate predetermined out-of-bounds conditions).

According to the National Archives and Records Service, General Services Administration (GSA), both types of controls are necessary and no automated decisionmaking application can be reliable if either type of control is deficient.

These applications use data originally prepared by people. The data input process often consists of people

- Filling out hard copy documents,¹ often on predesigned standard forms; and
- Converting the data to a form that can be read by the computer—machine-readable form.

As part of the external controls that should exist, the people doing the work should be qualified and adequately trained. Adequate guidelines should be given to these people on a timely basis instructing them how to fill out the documents involved, including what entries should be made under varying circumstances. The forms (hard copy and input) should be designed to be as simple as possible to allow for easy reading by people. Procedures should exist for reviewing (i.e., statistical sampling) input documents to test their completeness and accuracy. Controls should also provide for timely processing of the data.

If incomplete or inaccurate data enters the computer system undetected, automatic actions can be incorrect. The actions will continue to be incorrect if that data is stored in ADP files and reused. These applications can also make incorrect decisions if current data is not put into the system.

Causes of data problems

To identify some of the causes of the data problems, we:

- Contacted Federal officials at several agencies;
- Received responses to questionnaires from 205 individuals who are experienced in the area of data management in computers; and
- Analyzed causes cited by internal auditors.

A schedule summarizing some of the causes of data problems is followed by a discussion of each.

¹ Under some circumstances, such as source data automation and direct input devices, hard copy documents are not prepared.

Summary of Causes of Data Problems

Cause	Opinions of people answering the questionnaire --degree of causes (note a)		Identified from contacts with officials of Federal agencies (note b)	Cited as a cause by internal auditors
	Moderate to very large	Somewhat small or none		
Forms designed and used for input preparation are too complex.	183	21	x	
ADP files are not always adequately reviewed to assure that good data is being used.	178	26	x	x
Instructions to people preparing data input are not always provided, are provided late, or are not adequate.	175	30	x	x
Preparers of data input are not always adequately trained.	159	46	x	x
Manual reviews of input documents are not always adequate.	144	61	x	x
High volumes of transactions cause input preparers to make errors (workload pressures).	131	73	x	x

a/The questionnaire presented "some possible causes of the data conditions (problems) * * * " and asked that "based on your data management experience * * * indicate the degree to which you believe each of these causes contributes to the data condition (problems) in general." The responses allowed were to a: very large degree, somewhat large degree, moderate degree, somewhat small degree, or very small degree, or not at all.

b/Our contacts were made with various organizational elements, excluding internal audit, within six agencies: the Department of the Navy; Department of Health, Education, and Welfare; Veterans Administration; National Bureau of Standards; National Archives and Records Service; and Civil Service Commission.

The errors occur at the source of data preparation. They are not detected by the various internal controls in the software because controls for the specific error (1) are not designed or (2) cannot be designed.

Forms designed and used for input preparation are too complex

Using simple forms to record, collect, transmit, and process information for input to computers improves the completeness and accuracy of the data eventually used by all computer application programs. The more complex the forms are, the more prone they are to data errors, which can effect the correctness of actions initiated by automated decisionmaking applications.

ADP files are not always adequately reviewed to assure that good data is being used

A recognized external control technique is to output and review data contained in ADP files. Failure to do this can result in obsolete or otherwise incorrect data used in automated decisionmaking applications. Incorrect decisions are therefore initiated. Without reviews, it is possible for some data errors to remain undetected for years and to allow for an accumulation of errors compounding the problem.

Instructions to people preparing data input are not always provided, are provided late, or are not adequate

It is important to provide clear instructions to people preparing input documents. Timely updating of these instructions when changes occur is also important. The failure to issue clear and timely instructions can cause data errors that may not be detected by internal controls.

Preparers of data input are not always adequately trained

Most training in the input data preparation area is done by individual agencies, because it must be geared toward the individual application, each with its own special forms, data content, and related input media.

Inadequate training of persons involved in processing data to the computer (such as filling out forms and punching cards) can lead to high error rates which result in bad decisions made by these applications.

Manual reviews of input documents are not always adequate

External controls include selective manual reviews of input documents to determine completeness and accuracy. These reviews, made by supervisors or quality control groups, should be geared toward measuring the quality of data entering the system, including determining trends, significance, and sources of errors.

When there are different types and sources of input, review procedures should cover them all. Developing and monitoring statistical error rates is important. The review procedure, however, should also include determining the errors' potential materiality so that management can make judgments on where corrective actions should be taken.

Manual reviews supplement internal controls by (1) disclosing needed software data validation (such as edit checks) that is missed because of software problems or (2) identifying trends of material data errors which are not detected by software data validation.

High volumes of transactions caused input preparers to make errors (workload pressures)

Automated decisionmaking applications are designed, in part, to help organizations cope with the high volumes of transactions that have to be processed. Although the computer processes the data once it is entered, the volumes of documents (hard copy and machine readable) that must be prepared are tremendous. For example, we estimated that during a 12-month period, the VA Center, Philadelphia, Pennsylvania, prepared more than 4 million documents for input to computers. Other VA activities throughout the United States also prepare such input documents. The Navy Aviation Supply Office (ASO), also in Philadelphia, annually receives about 10 million transaction reports for input to computers. The transaction reports are mainly prepared by Navy facilities that receive, store, and issue aeronautical equipment.

The volumes of data that must be processed by people recording material on original documents and preparing machine-readable documents can lead to workload pressures that result in data errors.

CHAPTER 5

FEDERAL MANAGEMENT OF AUTOMATED DECISIONMAKING APPLICATIONS

Although we believe that most decisions made by these applications are correct, we know from audit reports we reviewed that they also make bad decisions that cost the Government many millions of dollars annually. Additionally, bad decisions can impede agency mission achievement and may result in harm to people.

To a large degree software design and data quality control are an art. Much of the process is imperfect because people instruct the computer and supply data to it.

The fact that computers will act only as instructed by people, and on data prepared by people, makes them particularly susceptible to incorrect output, which in an automated decisionmaking application causes incorrect actions.

Undetected errors in preparing the software—whether caused by the user, the designer, or the programmer—can cause the computer to repeat bad decisions. These errors will continue until the problem is detected and corrected.

Data problems may be random or repetitive. The repetitive problems resulting from such items as inadequate instructions and complexity of forms will also continue until corrective actions are taken.

RESPONSIBILITIES FOR ADP MANAGEMENT IN THE GOVERNMENT

Public Law 89-306, the Brooks Act, specifies the major ADP management responsibilities of the Office of Management and Budget (OMB), the General Services Administration (GSA), and the Department of Commerce.

Under this act, the Administrator of General Services is charged with economic and efficient purchase, lease, and maintenance of ADP equipment by Federal agencies. The Administrator also has some control over using ADP equipment. The Department of Commerce is authorized to provide scientific and technological services for ADP systems and to make recommendations concerning ADP standards. This is carried out through the National Bureau of Standards' Institute for Computer Sciences and Technology. The act states that the authority granted to the Administrator of General Services and to the Secretary of Commerce is subject to policy and fiscal control by OMB. This constitutes oversight responsibility for the area.

In response to Government needs for training and education in ADP, the Civil Service Commission's Bureau of Training operates an ADP Management Training Center. This center offers a variety of courses to Federal civil and military personnel. Certain portions of their curriculum address the controls area in automated systems. The

material presented should assist in alerting managers who take these courses to possible control weaknesses in their agency's operations.

No Federal-wide guidelines on automated decisionmaking applications

Neither GSA nor the Secretary of Commerce has considered these applications as a separate subject matter for management consideration. There are, therefore, no established Federal guidelines for identifying, developing, operating, or monitoring these applications to insure that they are operating effectively and economically.

POLICY ACTIONS BY FEDERAL AGENCIES TO MANAGE AUTOMATIC
DECISIONMAKING APPLICATIONS

No Federal agencies we contacted had considered these applications separately from other types of computer application programs in issuing management instructions. When instructions on software design had been issued, they were general and dealt with such things as:

- Levels of approval required to initiate and process a design project;
- Concepts of project management—including setting priorities, establishing target dates, and requiring cost-benefit studies;
- The phases of software design and the documentation required; and
- Testing and certification requirements.

Considering the current state of the art and the human problems that exist, we agree with those Federal officials who contend that issuing detailed instructions on how to design these applications (or other computer application programs) will not in itself materially reduce many of the errors that are made in them.

Inventories of automated decisionmaking applications

Agencies have done little to establish centralized information on computer application programs that identifies these applications and shows their characteristics. Characteristics include the (1) nature of actions initiated, (2) monetary and other impact on operations, and (3) nature and sources of input. Information is sometimes available within an agency but must be pulled together from different sources. This is done mainly when requested by higher level sources, such as headquarters, a budget committee, or an agency such as GAO. It is not normally done.

WHAT AGENCIES DO

We studied what Federal agencies do in designing, modifying, testing, and operating these applications. We also studied how these agencies manage data entered and contained in their computer. The studies were made at selected agencies of the Department of Defense (Navy), HEW (Social Security Administration), and VA (education and insurance applications). We also visited a responsible headquarters agency in the Department of the Air Force to discuss these subjects on a limited basis.

We examined policy and existing procedures and practices for managing computer application programs but did not verify that they were being employed as described to us.

Despite the apparent variances in the nature and types of policies and instructions issued, the same types of problems exist at these and other agencies.

Design and modification

VA had no written instructions for designing or modifying computer application programs. VA told us that it relied on written text material as a guide. VA has issued instructions on establishing and controlling software design projects, establishing approval levels, and establishing priorities and target dates.

The Social Security Administration (SSA) has issued a guide that describes the various phases of the design and modification processes, establishes review and approval steps, and describes who is responsible for doing the work.

Neither agency has issued instructions on how to do the design work or what to consider when doing such work. VA officials do not believe that it is necessary or even feasible to issue such instructions. SSA assumes that designers and programers are adequately trained and experienced since courses are continually offered so that skills can be maintained at a satisfactory level.

The Navy Fleet Material Support Office (FMSO) is the central design activity for Naval Supply Systems Command activities. They have issued instructions to designers and programers in the form of information processing standards. The instructions provide guidance on what designers and programers are supposed to consider when doing the work, including:

- Customer and mandated requirements;
- Logical sequencing of ADP actions;
- Types of input and output;
- Data formats and uses;
- Data accuracy, completeness, and currency requirements;
- Error and exception conditions (edit checks); and
- Data volumes and frequencies.

Independent reviews of designed and modified product

The reviews of the detailed designed product¹ are generally made by the user and/or the people doing the work. According to agency officials the extent of these reviews varies from

- A page-by-page analysis made by ASO of products designed by FMSO to
- A less formalized cursory review made by supervisors or management.

We observed no requirements for making independent reviews of the detailed designed product. Essentially, the people doing the work are responsible for doing the detailed reviews.

The Air Force Audit Agency independently reviews selected data processing systems before they are implemented (preimplementation reviews). These reviews, made at four Air Force design activities, include evaluating the designed computer application programs and related edit checks.

¹ Usually consisting of a narrative or flow-chart description of the processing to be followed by the computer during operation.

This approach requires the auditor to become familiar with functions supported by applications, as well as learning basic software design and data control concepts. It includes reviewing and evaluating (1) the decisionmaking criteria, (2) the program coding, (3) the edit checks, and (4) other potential data problems.

The Audit Agency had never calculated cost savings that resulted from identifying and correcting potential problems before the applications were placed into operation. A major reason cited was that since corrective actions were often taken on the spot, there was no need for estimating unnecessary costs that would otherwise have resulted during operation.

Preimplementation audit reports of the Air Force Audit Agency showed that many of the problems that had been reported in operational automated decisionmaking applications were identified during preimplementation reviews, and Air Force design officials agreed that the problems existed. For instance, reports showed examples of:

- Erroneous decisionmaking criteria;
- Programing errors; and
- Inadequate data controls.

We discussed the concept of independent preimplementation reviews with the Deputy Director of the Air Force Office of Data Automation. He agreed with the concept of such independent reviews but preferred that the reviews be made by independent teams within the design activity. He believes that auditors should become involved in evaluating designed or modified applications as soon as possible after the applications are placed into operation.

Despite not making a savings analysis on preimplementation changes, the Air Force Audit Agency believes that preimplementation reviews should continue because:

- The quality of data systems is improved as a result of Air Force Audit Agency reviews.
- The dollar impact of resources managed by many automated systems is a proper subject for special audit.
- Systems audits during the development stage help increase the auditor's knowledge of the systems.
- The ability to make effective and efficient follow-on audits of operations is enhanced by the preimplementation reviews.

Testing

After the designed or modified application program is coded, agencies test the logic to determine whether the program will run and will perform the processing desired by the user. A description of the nature of testing by each agency follows.

- Programers at the Navv FMSO prepare predetermined test cases and files to test the logic of the program. If the results are satisfactory, the user operates the program with a duplicate ADP file and a selected number of actual transactions, which varies with each application. Some of the selected transactions are traced to determine if the program is operating as intended and whether the decisions being made are the same as operating personnel would make under the circumstances. The user advises FMSO if there is a problem.

- Programers and designers at SSA test both test cases and actual transactions. The number of selected transactions will vary depending on the complexity of the program. The user is required to certify that the program is operating according to the user's requirements.
- VA primary testing is done by independent system auditors assigned to the Department of Data Management. The system auditors are independent of the programers and designers, although they also work for the same department. The system auditors use a large number of test cases that have been developed and reused during the years. An automated comparison of the processing is made before and after the logic changes, and the differences are printed out. Unless there are many differences all are reviewed for correctness. The cases that are not printed are not reviewed. The auditors must certify that the logic conforms to the user requirements or issue exception reports when it does not.

Federal officials recognize that the current state of the art in program testing is imperfect. According to Officials of the Institute for Computer Sciences and Technology of the National Bureau of Standards, most test procedures currently used do not insure that all lines of codes have been exercised. Officials at the agencies visited agree that it is virtually impossible to test for every condition, but say they do the best they can by

- Testing as many conditions as considered feasible and necessary and
- Adding to test case material conditions which caused problems during operations but had not been identified during the original test phase.

The Institute and the Air Force consider the test phase an area where the current state of the art must be advanced.

The Institute was aware of numerous examples of computer application programs which were considered to be adequately tested but which, during operation, ran into serious problems and caused incorrect actions. As a result, the Institute in cooperation with the National Science Foundation worked on methods to improve the state of the art.

One recently developed procedure is a software program that will monitor tests of computer application programs written in FORTRAN (a programming language). This program counts the number of times each line of code has been exercised by test cases. Even though there is no insurance that every conceivable condition will be tested, there is insurance that each line of code has been tested at least once. Until recently, this capability was not generally available.

In a February 1972 report, the Air Force said that software design and testing were the two most critical problems in ADP requiring further research and development. In July 1973 the Air Force entered into a contract for the development of the type of software device that the Institute had developed but for a different programming language.

Monitoring of program operation

VA and the Navy largely rely on (1) internal auditor's reviews and (2) feedback from people affected by bad decisions or operating personnel to identify automated decisionmaking application problems.

No formal systematic monitoring of the applications' output is made, with one exception; VA audits education payments to veterans in excess of a predetermined amount. We believe that this is of limited value in identifying many costly systematic problems in automated decisionmaking applications because some types of transactions will never be reviewed.

SSA has a formal monitoring group continuously taking random samples of automated decisionmaking application output. According to SSA officials, this sampling has identified design and programming errors and repetitive data errors causing erroneous payments in operating automated decisionmaking applications. Examples of the kind of errors identified by this monitoring function include:

- Design, coding, or data problems in the automatic computation or recomputation of initial or subsequent benefits.
- Data problems in processing notices which affect payments.
- Design or coding problems in the updating of master data records (ADP files).
- Inadequate preparation of data.

SSA told us that system design and coding errors, as well as systematic repetitive data errors, were corrected as a result of this procedure. However, it could not give us statistics on numbers of errors found or their potential monetary impact, because SSA did not have this kind of information.¹

SSA requires categorizing, in addition to monitoring, the reasons for required program modifications. The categories include:

- Incomplete or incorrect performance requirements or program specifications.
- Logic errors or program omissions.
- Incomplete validation of input data.
- System-produced data not in accordance with specifications.
- Incomplete testing.

HEW headquarters said that a consulting firm noted a need for continuing reviews and evaluations of, among other things, applications software. The firm suggested that a four-member team, including an auditor, be responsible for reviewing selected applications on a short-term cyclic basis including (1) reviewing the application against the original specification to determine that the software was performing as intended and (2) determining whether application programs had been adequately modified when the processing circumstances changed. HEW did not accept the firm's report.

Data control

The sources of data input vary for the following locations.

- Navy ASO, Philadelphia, receives much of its data from external sources including (1) contractors for new aeronautical equipment entering the supply system and (2) other Navy activities that receive, store, and issue aeronautical equipment.
- SSA, Baltimore, Maryland, receives most of its data from about 1,300 offices and centers throughout the United States.

¹ Monitoring procedures are not always carried out as soon as new programs are placed into operation. The supplemental security income program, an automated decisionmaking application, did not have full-scale monitoring during its initial operational periods.

—The VA data processing centers in Hines, Illinois, and Philadelphia, receive data from several VA stations throughout the country.

Internal controls

Our review shows that, even though written procedures may not exist, agencies develop and program extensive edit checks in software to help insure the validity of data coming into the system. Agency officials admit that, although extensive work is done to analyze potential data errors during the design process, edit checks cannot be designed to identify all types of data errors.

In many cases erroneous but acceptable data may be placed on input documents. Because such data can represent a valid situation, there may be no way to design an edit check to insure that it is correct. Also, edit checks will not catch errors not conceived of—and therefore not considered—in designing edits.

Agency officials agreed that, because of the detail and complexity involved in the design process, potential edit checks may be missed.

Examples of the types of checks observed at the three agencies visited included:

- Edit checks for incomplete data elements;
- Reasonableness checks; for example, rejected documents containing numerical values above or below a predetermined amount in a given data element;
- Logical checks; for example, checks for impossible conditions, such as negative inventory balances or alphabetic characters contained in data elements that were designed to contain only numeric characters; and
- Data relationship checks; for example, comparing data elements with other data on the same input document and/or contained in ADP files.

External controls

Because agencies receive input from numerous sources, we limited our study of external controls to the controls at the agencies actually visited (VA Center, ASO, and SSA).

- VA has written procedures for several external control functions which include (1) random sampling of input documents to identify and develop statistics which are used for identifying error rates and error sources, (2) selected verification of eligibility data contained in ADP files, (3) date stamping and sampling of documents to control the timeliness of documents processed, and (4) controls over unprocessed (pending) documents.
- ASO makes no manual reviews of supply-related data received from Navy activities and therefore primarily relies on (1) controls at the data preparing site and (2) internal controls designed in the ASO software. ASO makes selected manual reviews of data received from contractors on new aeronautical components before the data is allowed to enter the system.
- SSA basically relies on the (1) internal controls designed into the software, (2) end-of-line monitoring procedures, and (3) manual reviews at the vast numbers of offices and centers preparing the data.

CHAPTER 6

AUTOMATED DECISIONMAKING APPLICATIONS CONTINUE TO MAKE BAD DECISIONS UNTIL PROBLEMS ARE CORRECTED

Errors made by users, designers, and programmers of automated decisionmaking applications, if not identified and corrected in the review and testing phases of the design process, can cause bad decisions which will continue until the errors are detected and corrected. When an insignificant error for a given action is multiplied by thousands or millions of the same type of actions over a period of time, the error is compounded. Unnecessary costs will grow and become large. An error allowed to exist for 5 years will cost the Government more than if the error is detected and corrected within, for example, 3 months after the automated decisionmaking application is in operation.

ERROR DETECTION

In previous chapters we discussed what agencies do to detect design and data problems. Because errors get through design and test processes and because data errors are made, early detection of them is important in reducing the cumulative effects of bad decisions.

ERROR CORRECTION

Detecting errors occurring in automated decisionmaking application software and/or data will not, by itself, stop the unnecessary costs being incurred. When detected, action must be taken to correct the errors by modifying the software, or improving the data quality, or both.

We have noted some instances in which problems were identified but corrective actions were not taken for a long time. An example follows.

Navy use of overstated demands in automated decisionmaking applications

A GAO report, B-162152, May 21, 1974, noted that in 1969 Navy auditors saw a need to design a routine in the standard computerized supply management system used by Navy inventory control points for removing from ADP files past material usage quantities (demands) associated with canceled requisitions. The demands recorded in these ADP files were used by several automated decisionmaking applications.

The report noted that in 1969 Navy command officials agreed with the need to properly adjust demand forecasts for invalid orders but said that it would not be able to correct the problems before 1971 because of other priority work. The report said that, at the time of the GAO review in 1972, the Navy was still not eliminating from ADP files demands related to invalid orders.

We estimated that about \$34 million in invalid demands were in Navy ADP files and that these overstated demands resulted in unnecessary materiel buys and repairs totaling about \$10 million a year. At least \$3 million in annual unnecessary costs were initiated by automated decisionmaking applications using this overstated demand data.

The design change to correct the condition had not been made at the time of this review, so we discussed the reasons for the delay with appropriate Navy officials.

We were told that, because of the GAO report and direction received from the Department of Defense, a high-priority project was established on June 14, 1974, to make the needed design modification.

The reasons cited by Navy officials for the 5-year delay in initiating the modification included

- Disagreement within the Navy on whether all canceled requisitions should result in reducing recorded demands;
- High-priority workload at the design activity mandated by higher headquarters levels in both the Navy and the Department of Defense; and
- Lack of pressure placed on the Navy command and design activity by the inventory control points since reduced demands could result in budget reductions.

AGENCY PROCEDURES FOR TIMELY CORRECTION OF SOFTWARE DESIGN PROBLEMS

Agencies establish priorities and target dates for software design and modification projects. Agency guidelines also require cost-benefit studies to justify establishing and committing resources to a large design effort.

According to some Federal officials, however, little attention is given to doing cost-benefit studies which demonstrate either (1) how much will be saved by eliminating an automated decisionmaking application problem that exists or (2) how much the continuing automatic decisions will cost the Government if the problem is allowed to go unchanged.

CHAPTER 7

OPINIONS ON WAYS TO PREVENT OR REDUCE THE IMPACT OF PROBLEMS IN AUTOMATED DECISIONMAKING APPLICATIONS

We believe that, despite the imperfect state of the art in application design and the widespread problems of getting quality data to the computer, every Federal agency using these applications should consider doing certain things to prevent or reduce the impact of the problems identified in this report.

We issued a questionnaire to 200 members of each of the following professional associations that are dedicated to furthering the quality of ADP-produced products:

- The Association for Computing Machinery's Special Interest Group for Business Data Processing.
- The Association for Computing Machinery's Special Interest Group for Management of Data.
- The Society for Management Information Systems.

The questionnaire described the various problems that we had observed in both the software design and data areas and requested the members to rate possible solutions presented in terms of their effectiveness and cost benefit. The ratings were designed to determine the validity of each solution, assuming each application involved spending millions of dollars or had an impact on people.

Some of the solutions can be applied before the application becomes operational to prevent problem conditions. Some of the solutions were to be applied after the automated decisionmaking application became operational to detect problem conditions early. If timely correction is made, the impact will be reduced.

A total of 263 people responded to the questionnaire.

SUMMARY OF PEOPLE ANSWERING THE GAO QUESTIONNAIRE

Affiliation of data processing professional	Portion of questionnaire qualified to answer—			
	Design and data	Design only	Data only	Total
Commercial concern.....	136	45	4	185
Academic.....	34	10	1	45
Government.....	25	1	1	27
Not indicated.....	4	2	0	6
Total.....	199	58	6	263

POSSIBLE SOLUTIONS—SOFTWARE PROBLEMS

Some of the highly rated solutions to the various design conditions are:

- Documentation should be prepared that highlights (1) key portions of the automated decisionmaking criteria, (2) data elements that are critical to the decisionmaking, and (3) the edit checks placed (or justifications for omitting them) in the software. A formalized synopsis of these items should be prepared for review and approval by top management.
- Qualified auditors or others who are independent of designers and users should review the designed application before it is placed into operation. Others could include a design team independent of the original designer and user. They would be responsible for evaluating the (1) adequacy of the decisionmaking criteria, (2) logic in the coded application, and (3) needs and uses of edit checks to detect incomplete data elements put into the application.
- Similar independent teams should review the operation of these applications shortly after they are implemented. The objectives would be to evaluate the adequacy of the decisionmaking criteria in an operational environment and to provide for early detection of any bad decisions. This would allow for early correction of problems.
- Some form of cyclical system monitoring of actions initiated by operational automated decisionmaking applications should exist. Teams composed of (but not restricted to) designers, users, and auditors could analyze application-initiated actions to (1) see if desired results were achieved the best way, (2) identify unforeseen circumstances that would require modifying the application, (3) determine that the actions were as the user and designer intended, and (4) insure that decisionmaking was not adversely affected by incomplete data not being screened by an edit check.
- The designer and user should be physically located in the same place during design phases to allow for constant communication. In effect, the design would be a joint effort and would help to insure that adequate decisionmaking criteria were contained in the application.
- Priorities should be established for software modification (changes) which are at least partially based on the cost of continuing incorrect automatic actions if no changes are made within a short time.
- The initiator of the needed software modification (for example, headquarters, user, audit team, and/or others) should be informed about the status of the change and be provided with confirmation that the changes have been made.

POSSIBLE SOLUTIONS—DATA PROBLEMS

Some of the highly rated solutions to the various data conditions are to:

- Establish followup procedures for insuring the (1) timely receipt of data preparation instructions and (2) use of instructions by data preparers.
- Emphasize in training the importance of complete and correct data on computer input documents.

- Make selective manual verification of key data on input documents and in ADP files with hard copy documents and with the data originator.
- Establish a single organization (data base administrator) that could be responsible for the above steps as well as evaluating and testing internal and external data controls employed and input documents designed and used.

CHAPTER 8

CONCLUSIONS, RECOMMENDATIONS, AND AGENCY COMMENTS

Automated decisionmaking applications initiate the spending of billions of dollars a year without anyone reviewing and evaluating the individual actions. They are also used to support a multitude of functions that, although not directly related to money expenditures, can affect mission achievement and make decisions regarding individuals.

Many of these applications make bad decisions because of various software and data problems. The causes of the problems are numerous. Bad decisions may result in unnecessary costs and overpayments of hundreds of millions of dollars a year—exactly how much is unknown. Such bad decisions can also impair mission performance and harm individuals.

In the current imperfect environment, the chances of continuing bad decisions and unnecessary costs are great. Actions are needed. We believe that it is necessary therefore to develop and issue Federal-wide guidelines to foster uniform cost-effective practices that will (1) minimize the chances of problems occurring, (2) detect as soon as possible the problems that do occur in operating automated decisionmaking applications, (3) correct problems as early as possible to reduce their adverse impact, and (4) insure that the practices are being effectively applied.

Some practices we consider necessary to meet these objectives already exist at some agencies. For instance, we observed testing, joint design, and inclusion of internal data controls. We also observed some established data management practices which could identify data input problems.

Several practices considered by us and by data processing professionals to be cost effective in reducing the chances or impact of bad decisions were not being applied to all crucial automated decisionmaking applications. This indicates a need for central guidelines in such areas as:

- Preparing documentation and/or a formalized synopsis that highlights, for example, key decisionmaking criteria, data elements critical to the decisionmaking, and edit check placement to facilitate thorough reviews by others.
- Making preimplementation reviews of the designed or modified applications and internal data controls. The reviews should be made by groups that are independent of the designer or user. The groups should consider evaluating, among other things, the (1) adequacy of the decisionmaking criteria, (2) logic in the coded application, and (3) needs and uses of edit checks contained in these applications.

- Analyzing actions initiated by these applications as soon as possible after they are placed into operation to insure that (1) they are operating as intended, (2) the intended operation is the most economical and effective method, and (3) circumstances that were not considered during design have not arisen.
- Cyclical or ongoing monitoring of automated decisionmaking application output to insure that (1) desired results are achieved most economically and effectively, (2) new circumstances have not arisen that will require changes to the decisionmaking or other processing criteria, (3) the logic is correct, and (4) decisionmaking is not adversely affected by incomplete data not being caught by an internal edit check.
- Establishing priorities and target dates for software modification which are at least partially based on the unnecessary costs of continuing incorrect automatic actions and keeping the initiator of modifications informed of the status of the changes.
- Establishing a single point in each organization that would have prime responsibility for insuring that these applications are making decisions based on the best data available by (1) evaluating and testing the data and data controls (internal and external), (2) adequately training data preparers, (3) reviewing the adequacy and currency of instructions given data preparers and insuring they are complied with, and (4) insuring that forms designed for data processing minimize the chances of data errors.

To begin focusing on what should be managed, top management in each agency should be aware of the automated decisionmaking applications that exist (operational and under development), the functions they support, their monetary and other impacts, nature and sources of input, the output-initiated actions, the programmed reasons for any manual intervention, and other important characteristics.

Agencies should be required to take stock of their automated decisionmaking applications. This action should include ascertaining whether their current practices for developing, modifying, and operating such applications, together with related data controls, are adequate to surface problems of the types discussed. Guidelines should be issued to indicate cost-effective corrective procedures, and agency management should insure that automated decisionmaking applications are under control.

RECOMMENDATIONS

We believe that, since automated decisionmaking applications have not previously been recognized as a separate problem area requiring management attention and since millions of dollars are presently being wasted as the result of actions generated by such systems, the Office of Management and Budget (OMB) should act immediately to improve the situation. Specifically, we recommend that OMB, in its oversight capacity, require that :

- Each agency determine whether any of its computer operations involve automated decisionmaking applications.
- The agencies review each operation to determine whether incorrect actions are being taken as a result of these applications. (Pending issuance of technical guidelines by the National Bureau

of Standards for making such reviews, the agencies should examine enough automatically generated decisions to provide a basis for deciding whether incorrect decisions are occurring and, if so, should take the necessary steps to correct the situation causing the incorrect decisions.)

- Before any new automated decisionmaking applications are initiated by an agency, the proper steps are taken to insure correct decisions. This would include, pending issuance of the National Bureau of Standards guidelines, a carefully chosen combination of independent review of systems design, adequate testing before implementation, and periodic testing of decisions after implementation, as discussed earlier in this report.
- Agencies report on the actions taken and establish an appropriate mechanism for monitoring such reports.

We recommend that, because the National Bureau of Standards has responsibilities for technical aspects by ADP, the Secretary of Commerce direct the Bureau to issue technical guidelines for developing, using, technically evaluating, documenting, and modifying these applications in the Federal Government. When issued, these guidelines should contain certain criteria for independent technical reviews and for monitoring of these applications to insure problems are detected and corrected promptly. The General Services Administration should incorporate Bureau guidelines in its agency directives.

In addition, we recommend that:

- As GSA suggested, the Civil Service Commission develop and add to its ADP training curriculum courses in automated decisionmaking applications so that managers, technical personnel, and auditors will become better equipped to deal with them in an appropriate manner.
- Internal audit groups in agencies having automated decisionmaking applications participate actively in design, test, and reviews of such systems to carry out their responsibilities.

Finally, we suggest that the Joint Financial Management Improvement Program consider this area for ongoing attention.

We are sending copies of this report to all departments and independent agencies for their information, use, and guidance pending issuance of the OMB and National Bureau of Standards material.

AGENCY COMMENTS

We issued the proposed report to several agencies for comment. Their replies indicate general agreement as to the problems reported and varying opinions on the recommendations.

With respect to the problems, the Associate Deputy Administrator, VA, agreed that there was a need for sound management of current large sophisticated data processing systems. He said the report was useful in identifying and consolidating the problems associated with automated decisionmaking applications. He believes that the formulation of standards relating to these applications is imperative.

The Assistant Secretary, Comptroller, HEW, said that no one would disagree that software and data problems exist and that such problems could result in automated decisionmaking applications that

made erroneous decisions in some cases. He believed that as much emphasis should be placed in preventing software errors as in detecting and correcting them. He agreed that the current state of the art in software development could not assure error-free software.

The Assistant Secretary of Defense, Comptroller, said that most of DOD's automated systems fit the definition of automated decision-making applications, although damage resulting from errors in some systems was less direct and less measurable than in disbursing and supply systems. He added that our statements of possible solutions to software and data problems are logical and constructive and that while they are similar to many DOD practices, their documentation will assist system developers, auditors, and operators.

The Acting Administrator, GSA, said that the report performed a valuable service in identifying automated decisionmaking applications as an area of data processing concern and, as such, warrants wide circulation to ADP software managers in the Federal Government. He strongly agrees with our solutions for software and data problems, including:

- Preimplementation and postimplementation system reviews by independent groups; and
- Cyclical system monitoring.

The agencies had varying opinions on the tentative proposals contained in our proposed report. We have weighed their comments and considered them in formulating the proposals in this report. For example, we proposed that the agencies involved report to GSA on actions taken in response to our recommendations. Upon consideration of the responses to our proposed report, we have modified our recommendation to provide for OMB to determine an appropriate reporting mechanism.

Also in response to our proposed report, the Acting Administrator, GSA, suggested that the National Bureau of Standards could develop Government-wide guidelines for information systems development which could specifically include automated decisionmaking.

On January 12, 1976, we discussed the suggestion with the Director, Institute for Computer Sciences and Technology, National Bureau of Standards, who agreed to the need for Government-wide technical guidelines that would include developing, using, modifying, reviewing, and monitoring automated decisionmaking applications and said that budgetary resources would be solicited for the National Bureau of Standards to perform this task. The guidelines, when completed, would be issued as part of the Federal information processing standards series for use by Federal agencies.

We informally discussed the recommendations with OMB officials who have responsibilities in the ADP area. They believe that the report points out important problems in this area and agree that issuing policy guidance is appropriate.

We discussed our recommendations to the Civil Service Commission with officials of the ADP Management Training Center who agreed to further emphasize controls in their ADP training.

APPENDIX I

APPENDIX I



DEPARTMENT OF HEALTH, EDUCATION, AND WELFARE
OFFICE OF THE SECRETARY
WASHINGTON, D.C. 20201

NOV 17 1975

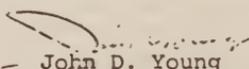
Mr. Gregory J. Ahart
Director, Manpower and
Welfare Division
U.S. General Accounting Office
Washington, D.C. 20548

Dear Mr. Ahart:

The Secretary asked that I respond to your request for our comments on your draft report to the Congress entitled, "Improvements Needed in Managing Computer-Based Automated Decisionmaking Applications in the Federal Government." They are enclosed.

We appreciate the opportunity to comment on this draft report before its publication.

Sincerely yours,


John D. Young

Assistant Secretary, Comptroller

Enclosure

COMMENTS ON GAO'S DRAFT REPORT ENTITLED
"IMPROVEMENT NEEDED IN MANAGING
COMPUTER-BASED AUTOMATED DECISION MAKING
APPLICATIONS IN THE FEDERAL GOVERNMENT"

OVERVIEW

The draft report identifies a certain type of EDP application which GAO calls an Automated Decision Making Application, (ADMA), and notes that ADMAs are widely used by Federal agencies. The report points out that the distinguishing characteristic of ADMAs, as compared to other computer application programs, is that many of the actions initiated by the computer take place without review and evaluation by people. According to GAO, there are indications that funds are being wasted because of incorrect, unreviewed actions.

The report discusses, at some length, the use of ADMAs by Federal agencies, and points out that ADMAs can make bad decisions. It categorizes the causes of these bad decisions as being software problems or data problems, then goes on to identify and discuss the reasons for these problems.

No one will disagree that software and data problems do exist, and that such problems can result in ADMAs that make erroneous decisions in some cases. It is of utmost importance, therefore, that such problems be prevented during the design and implementation of the system. While we are of the opinion that the current state of the art in software development techniques and test techniques cannot assure that error free software can be designed, techniques are available that can contribute significantly to the reduction of software errors. Furthermore, practice has suggested that the method of organization of a development effort can have a favorable impact on the error level as well as the development cost.

Since the state of the art of development and testing techniques cannot assure error-free software, it is of equal importance that reviews of systems take place before operation, shortly after implementation, and on continuing or cyclical basis for operational systems. The extent of review of an ADMA should be a function of the probability and impact of errors.

The report discusses various ways to prevent or reduce the impact of problem conditions in ADMAs. In our opinion, the possible solutions mentioned in the report are, for the most part, reasonable. We would, however, place a greater emphasis than made in the GAO report on (1) involvement of the user in the development of an ADMA and (2) approaches to reducing probability of errors at the design and test stages rather than emphasizing error detection and correction in the operational stage.

GAO concludes that the development and use of ADMAs is necessary but because of the current imperfect environment, chances of continuing bad decisions and unnecessary costs are great. Consequently, GAO believes that it is necessary to develop Federal-wide policy to foster uniform cost-effective practices that will minimize the chances of problems occurring, detect the problems as early as possible, and assure that the practices are being effectively applied.

GAO RECOMMENDATIONS AND HEW COMMENTS

RECOMMENDATIONS

Because GSA is responsible for developing Government-wide policy on ADP management and for seeing that the policy is carried out by the departments and agencies, GAO recommends that the Administrator, GSA:

- Require the identification and characterization of ADMAs used by Federal agencies. (A starting point for material to be included can be the types of data GAO obtained during its study of ADMAs -- volume of transactions, impact of decisions, etc.). This will provide agency management and auditors with basic information on where their resources could best be applied.
- Issue policy requirements and guidelines for the management of ADMAs in the Federal government. Most importantly, the policy and guidelines should establish criteria for independent reviews and monitoring of ADMAs to assure that problems are detected and corrected in a timely manner. The policy should also include criteria for cost-effective development, modification, documentation, review and testing of ADMAs.
- Require agency reporting concerning (1) actions taken based on the criteria and (2) problems identified and corrected as a result of independent reviews and monitoring of ADMAs. Justification of cost effective ways of managing ADMAs should be included.

HEW COMMENTS

With respect to GAO's first recommendation, we do not believe that it would be useful to have all agencies identify and characterize their ADMAs. To do so would result in the preparation of an enormous volume of reports covering hundreds of ADMAs. Since it is unlikely that GSA would be

able to effectively utilize these reports, their development and preparation would be a waste of agency time and resources. For similar reasons, we do not favor GAO's third recommendation which would require agencies to submit reports concerning the actions taken pursuant to GSA policy directives.

We agree in principle with the second recommendation -- that GSA establish guidelines for the management of ADMAs in the Federal Government. The establishment of guidelines would encourage agencies to utilize acceptable practices for developing, modifying, reviewing and monitoring their ADMA systems.

We are of the opinion that such guidelines as GSA might develop must be flexible to recognize that ADMA systems are of varying complexity and of varying impact in terms of probability and cost of errors. Thus, practices employed for the development, modification, review, and monitoring of a particular ADMA should be oriented towards overall cost reduction, i.e., expected cost of errors plus cost of development, modification, ... In light of the diversity of ADMAs, we do not believe that it is practical to establish "policy requirements" at this time. We believe that a more effective procedure would be for GSA to issue guidelines and then to periodically conduct on-site reviews and audits of various agency ADMAs. The objective of such review would be twofold: (1) determination of the extent to which guidelines were being followed by agencies and (2) determination of the effectiveness and efficiency of the recommended practices so that they could be developed and refined based on actual experience.

Furthermore, as we indicate in the Overview to these comments, we believe that efforts to eliminate errors during development is of equal importance to the review and monitoring efforts. Therefore, we suggest modifying the second recommendation to read:

"Issue guidelines for the management of ADMAs in the Federal Government. These guidelines should include recommended practices and criteria for cost effective:

1. development, modification and testing of ADMAs to reduce error levels in software and data collection,
2. documentation of ADMAs for internal and external uses,
3. review and monitoring of ADMAs both as continuing activities by systems and user personnel and by independent groups."

OTHER COMMENTS AND SUGGESTIONS ON THE REPORT

1. In the third paragraph on page 58 of the draft report, a statement is made that "An SSA official said that they assume that designers and programmers are adequately trained and experienced and that such instructions are not necessary." This is not an accurate statement. We suggest that GAO change the sentence to read:

"An SSA staff member said that designers and programmers are adequately trained and experienced since there are continuing courses offered in systems design so that skills can be maintained at a satisfactory level."

2. In the last paragraph on page 65, the second sentence reads "According to SSA officials, this sampling has identified many design and programming errors and repetitive data errors causing erroneous payments in operating ADMAs." The word "many" is misleading in that this is an end of the line operation and most errors are discovered in validations, etc. long before these operations are performed. The sentence should read:

"According to SSA staff members, this sampling has identified design and programming errors and repetitive data errors causing erroneous payments in operating ADMAs."

3. The first paragraph on page 66 begins "SSA advised us that many system design and coding errors, as well as systematic repetitive data errors, are corrected as a result of this procedure." For the same reasons given in the preceding paragraph of our comments, the word "many" is misleading and should be deleted.

5. There is considerable overlap and duplication in several chapters of the report. In particular, we suggest that Chapters 3 and 4 be combined to improve readability.

6. We believe, in general, that the report tends to underplay the importance of the user in the development of an ADMA. We note with interest that in the opinion of "people answering the questionnaire" (page 36 of the report) the most often cited problem is "inadequate communications between the parties to software design." The second ranked problem in this list is "incorrect perceptions of the nature of the actual transactions to be processed."

Furthermore, in Chapter 7, "Opinions on ways to prevent or reduce the impact of problem conditions in ADMAs," respondents from several professional organizations suggest that "Physical collocation of the designer and user should be accomplished during the design phases to facilitate constant communication. In effect, the design would be a joint effort and would help to insure adequate decision-making criteria contained in the ADMA." Despite the importance of these causes of errors and of this recommendation of professionals to overcome them, the policies advocated by GAO in Chapter 8 fail to address the necessity of user involvement.

Therefore, we suggest that the GAO report place greater emphasis on the participation and responsibility of the user in an ADMA system. In commenting on the draft GAO report "GAO Guidelines for Management Information Processing Systems," May 1974, HEW stated: "The Guidelines include the user in the system development from the standpoint of user education as opposed to user participation. While user education is important, it is not enough. The success or failure of a system is critically dependent on user involvement and participation." We believe that this dependency is even more critical in an ADMA system.

7. The importance of personnel selection and training for ADMA development, operation, monitoring and review should be given greater emphasis in the GAO report. Designers and programmers should be familiar with design tools and techniques, e.g., structured and modular flowcharting and programming, decision tables, data base design tools, data element management, data collection alternatives. Management should be aware of alternative organizations for system development, e.g., chief programmer teams. Designers should also be aware of techniques for testing and monitoring systems including statistical sampling approaches. Knowledge can be obtained via government or private sector training courses.

GAO note: Material no longer related to report has been deleted.

APPENDIX II

APPENDIX II



VETERANS ADMINISTRATION
 OFFICE OF THE ADMINISTRATOR OF VETERANS AFFAIRS
 WASHINGTON, D.C. 20420
 NOVEMBER 28 1975

Mr. Gregory J. Ahart
 Director
 Manpower and Welfare Division
 U.S. General Accounting Office
 Washington, D.C. 20548

Dear Mr. Ahart:

We appreciate the opportunity to review and comment on your draft report relating to the management of automated decision-making applications and are in agreement that there is a need for sound management of the large, sophisticated data processing systems in existence today.

[See GAO note.]

Your report has proved useful in identifying and consolidating, in one place, many of the problems associated with automated decision-making applications in a clear, straightforward language. We believe that the formulation of standards relating to these applications is imperative, and have already begun to draft our own general requirements and guidelines.

Sincerely yours,

[Signature]
 Associate Deputy Administrator - in the absence of

RICHARD L. HOUEBUSH
 Administrator

GAO note: Deleted comments refer to material discussed in our draft report but not included in this final report.

APPENDIX III

APPENDIX III

UNITED STATES OF AMERICA
 GENERAL SERVICES ADMINISTRATION
 WASHINGTON, DC 20425



DEC 29 1975

Honorable Elmer B. Staats
 Comptroller General of the United States
 General Accounting Office
 Washington, D. C. 20548

Dear Mr. Staats:

We appreciate the opportunity to review your draft report "Improvements Needed in Managing Computer-Based Automated Decisionmaking Applications in the Federal Government."

The report performs a valuable service in identifying automated decision-making applications (ADMAs) as a discrete area of data processing concern and, as such, warrants wide circulation to ADP software managers in the Federal Government.

We strongly agree with the following GAO recommended solutions for software and data problems:

- Pre-implementation and post-implementation system audits by independent groups.
- Cyclical system monitoring.
- Joint system design by users and ADP systems analysts.

In addition to the management solutions mentioned in the report, there are modern computer programming techniques which can aid in increasing the integrity of any system. Developing detail logic with decision tables rather than flow charts is particularly effective in data editing applications. The use of "top down" programming and "chief programmer teams" is proving successful in minimizing errors. Employment of a data base administrator throughout both the developmental and operational stages of a system will help assure that valid data is being processed.

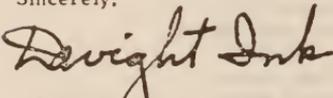
While we generally agree with the conclusions and recommended solutions for software and data problems contained in the report, we do not agree with the recommendations that GSA issue policy and guidelines for the management of ADMAs nor that GSA require agency reporting to allow monitoring of agency performance. Rather we would suggest, since ADMAs are part of the broader universe of information systems development, that:

- . The National Bureau of Standards, with GSA cooperation, develop government-wide guidelines relating to information systems development which should specifically include automated decisionmaking.
- . Agencies report to their own agency head regarding decision-making criteria, ADMA problem identification and corrective actions taken, and that these reports be made available for review by OMB and GSA, in line with review provisions in Federal Management Circular 74-5.
- . The Civil Service Commission include in its management training programs a course on automated decisionmaking stressing the need for cost effective development, joint systems design by users and ADP systems analysts, systems monitoring and auditing of ADMAs.

Because of the significance of this report, we had the opportunity to have the Ad Hoc Committee for Implementation of P. L. 89-306 briefed by a representative from GAO prior to issuance of this draft. This Committee is chaired by the Commissioner, ADTS, and representatives from ADP-intensive agencies are committee members. At a later meeting, our comments were discussed and the Committee generally concurred in the approach GSA is proposing.

If you have any questions, please let us know.

Sincerely,



Dwight A. Isak
Acting Administrator



ASSISTANT SECRETARY OF DEFENSE
WASHINGTON, D. C. 20301

COMPTROLLER

2 JAN 1976

Mr. Donald L. Scantlebury
Director, Division of Financial &
General Management Studies
U.S. General Accounting Office

Dear Mr. Scantlebury:

The Secretary of Defense has asked me to respond to your proposed report on managing automated decision making by computers in the Federal Government (OSD Case #4117).

The report sets out automated decision making applications (ADMA) of computers as a problem of unique major proportions because their outputs are not reviewed by humans. The implication is that this characteristic causes much greater risk of dollar losses and requires special management attention. Within DoD, most of our automated systems fit the definition, although damage resulting from such systems are less direct and less measurable than in purchasing and supply systems.

The systems management effort within DoD has for some years taken a multidisciplinary approach. Responsibility is placed on functional users of systems to specify their functional algorithms precisely, to accept responsibility for their documentation, and to participate in rigorous pre-implementation and prototype tests. Data automation personnel are subjected to quality control of systems modules during development, testing, and initial operations. Internal auditors are encouraged to provide advisory assistance to systems development personnel, particularly with respect to such aspects as internal controls and audit trails. DoD training activities and professional meetings of both audit and ADP personnel stress the importance to our mission effectiveness and resource control of constant and continuing quality control. The many quotations of DoD internal audit findings in your draft report testify to our active program.

In addition we are participating, as is your office, in the current research project of the Institute of Internal Auditors on "Systems Auditability and Control." We look forward to their findings for additional assistance in this area of mutual concern.

APPENDIX IV

APPENDIX IV

Because of the unique problems of automated systems, we have and will continue to develop and apply special measures to their quality control. However, they are in no way exempt from standard Federal accounting system certification, management reviews, and internal audit controls. The net effect then is to increase management control of automated systems in comparison to manual systems.

Your statements of possible solutions to software and data problems are logical and constructive. While they are similar to many DoD practices, their documentation in a compact set will assist our system developers, auditors and operators.

With respect to the recommendations included in the draft report, we interpret GSA's charter in the ADP field to address procurement of ADP equipment, supplies and services. Your report is aimed at a different arena, that of functional procedures and accounting controls. Accordingly, we recommend that:

1. The subject be proposed as a matter of continuing interest by the Federal Financial Management Improvement Program. The inter-agency effort of senior financial managers is an appropriate forum for exchange of new procedures and techniques.

2. Pertinent and documented studies, research reports, methods and techniques be provided by developing agencies to the National Technical Information Service (NTIS) of the Department of Commerce for dissemination at cost to other potential users in accordance with the NTIS charter.

3. The report be issued as a study, retaining the findings and conclusions but deleting the recommendations and substituting the following:

"Each Federal Agency should review its internal regulations and procedures for management of ADMA systems to assure protection of mission effectiveness and government resources from system errors. Each agency should establish specific internal procedures to assure that internal controls and audit trails for error detection and correction are made a part of system design specifications, tested prior to system implementation, and included in routine and special audits throughout their operational life."

APPENDIX IV

APPENDIX IV

Thank you for an informative and valuable research effort. The opportunity to comment on the draft report is appreciated.

Sincerely,

Terence E. McLaughlin

INTERNAL AUDIT REPORTS ON
AUTOMATED DECISIONMAKING APPLICATIONS

Title of report	Date	Type of application involved	Problem identified	
			Software	Data
Army Audit Agency: Coordinated Audits of Depots (Maintenance Operations)	3/ 4/74	Maintenance workload acceptance	X	X
U.S. Army Training Center, Infantry and Fort Polk	12/21/73	Requisitioning	X	
Direct Support System	10/16/73	Requisition processing	X	
Materiel Obligation Validation Procedures	2/ 8/74	Procurement cancellation	X	
Catalog Function	8/21/73	Automated procurement and requisition processing	X	X
Naval Audit Service: Servicewide Audit of the Aeronautical Repairable Components Program	12/ 6/73	Overhaul scheduling	X	X
Headquarters, Pacific Missile Range, Point Mugu, California	11/ 1/73	Requisitioning	X	
Navy Aviation Supply Office, Philadelphia, Pennsylvania	10/16/72	Redistribution	X	X

APPENDIX V

APPENDIX V

Title of report	Date	Type of application involved	Problem identified	
			Software	Data
Naval Audit Service (continued):				
Aviation Supply Office, Philadelphia, Pennsylvania	6/15/72	Requisition processing and redistribution	X	
Navy Aviation Supply Office, Philadelphia, Pennsylvania	12/10/74	Overhaul scheduling and redistribution		X
Auditor General, Defense Supply Agency: Physical Inventory Procedures and Practices	11/24/72	Physical inventory requests	X	
Medical Supply Functions	9/ 5/73	Customer returns, requisition processing and stock attrition	X	
Mobilization Reserve Requirements at Defense Supply Centers	5/18/73	Customer returns	X	
Veterans Administration, Fiscal Audit: Audit of On-Job and Apprenticeship Training Awards Processed by OCR	5/ 8/74	Payments	X	X
Processing Dependency Changes from Supplemental Award Code Sheets	9/17/73	Payments	X	

APPENDIX V

APPENDIX V

<u>Title of report</u>	<u>Date</u>	<u>Type of application involved</u>	<u>Problem identified</u>	
			<u>Software</u>	<u>Data</u>
Veterans Administration, Fiscal Audit (continued):				
Processing Awards after Entitlement is Exhausted	8/ 2/73	Payments	X	
Nonrecovery of Accounts Receivable from Resumed BCL Account Payments	4/20/73	Payments	X	
Retroactive Payment Adjustments	8/31/73	Payments	X	
Updating Accounts Receivable Deduction Amount from Amended Awards	4/12/73	Payments	X	
Duplicate Chapter 34 Education Payments	8/ 2/74	Payments	X	
Interior, Office of Survey and Review, Audit Operations:				
Review of Contract No. N00C14205253 With the Navajo Tribe, Window Rock, Arizona, Bureau of Indian Affairs	10/29/73	Payments	X	
Agriculture, Office of Inspector General:				
Programs Option B Provisions of the 1972 Feed Grain Set-aside Program	10/25/73	Payments	X	

APPENDIX V

APPENDIX V

Title of report	Date	Type of application involved	Problem identified	
			Software	Data
Agriculture, Office of Inspector General (continued):				
Loading Order Issuance Processing and Settlement	8/ 8/73	Loading order settlement	X	X
Agriculture, Office of Audit:				
Automated Accounting Service	2/15/74	Payments and billings	X	X
HEW Audit Agency:				
Administrative Costs Incurred and Benefit Payments Made Under the Health Insurance for the Aged Act	1/ 9/74	Payments		X
Administrative Costs Incurred and Benefit Payments Made Under the Health Insurance for the Aged Program	12/28/73	Payments		X
Administrative Costs Proposed and Operations Relating to Benefit Payments Under Medicare	6/28/74	Payments	X	
Administrative Costs Claimed and Benefit Payments Made Under the Health insurance for the Aged Program	5/24/74	Payments		X

APPENDIX V

APPENDIX V

Title of <u>report</u>	<u>Date</u>	Type of application <u>involved</u>	<u>Problem identified</u>	
			<u>Software</u>	<u>Data</u>
HEW Audit Agency (continued):				
Administrative Costs claimed and Supplementary Medical Insurance Benefit Payments Made Under Health Insurance for the Aged Program	11/ 9/73	Payments		X
Administrative Costs and Bene- fit Payments Under the Health Insurance for the Aged Program	11/12/73	Payments	X	X
Administrative Costs Claimed and Benefit Payments Made Under the Health Insurance for the Aged Program	5/ 1/73	Payments	X	X
Administrative Costs and Benefit Payments Made Un- der the Health Insurance for the Aged Act	4/12/74	Payments		X

**REPORT TO THE CONGRESS BY THE COMPTROLLER
GENERAL OF THE UNITED STATES—APRIL 27, 1976**

COMPUTER RELATED CRIMES IN FEDERAL PROGRAMS

Computer systems have added a new dimension for potential crime. Information on computer-related crimes in Government is difficult to gather, because they are not classified as such by investigative agencies. But GAO has learned of 69 instances of improper use of computers in Federal programs resulting in losses of over \$2 million.

Most of the cases GAO examined did not involve sophisticated attempts to use computer technology for fraudulent purposes; rather, they were uncomplicated acts which were made easier because management controls over the systems involved were inadequate.

Management needs to pay more attention to the importance of these controls.



COMPTROLLER GENERAL OF THE UNITED STATES
WASHINGTON, D.C. 20548

B-115369

To the President of the Senate and the
Speaker of the House of Representatives

Computer systems offer new methods for potential criminals to commit crimes. This report summarizes our study of Government crimes in which the perpetrators used computer-based systems. Our review was initiated because an increasing number of computer-related crimes had been discovered in the private sector of the economy, and we wanted to determine if they were occurring in Government as well.

We made our review pursuant to the Budget and Accounting Act, 1921 (31 U.S.C. 53), and the Accounting and Auditing Act of 1950 (31 U.S.C. 67).

We are sending copies of this report to the heads of Federal departments and agencies.

A handwritten signature in cursive script that reads "Louise R. Staats".

Comptroller General
of the United States

DIGEST

Computer systems have added a new dimension for potential crime. Computer-related crimes in Federal programs are cause for growing concern.

Information on computer-related crimes is difficult to obtain, because the crimes frequently are not classified as such by investigative agencies. Even so, GAO has learned of 69 crimes or other incidents resulting in losses of over \$2 million. (See app. I.) In addition to the dollar loss to the Government, some crimes violate the privacy of individuals about whom computerized records are kept.

Contrary to widespread belief, most of these acts have been committed by persons who possess limited technical knowledge of computers—that is, by users of automatic data processing systems rather than by persons with more technical knowledge such as programmers, operators, or analysts.

GAO found that management controls over the systems involved in crimes were inadequate. More attention needs to be paid to the importance of these controls.

One way for managers to insure that systems are properly controlled is to use internal audit staffs effectively. Auditors can identify control weaknesses that may result in criminal activity. But they must have adequate training, and they should evaluate controls as systems are being designed as well as review systems in operation.

GAO recommends that the heads of Federal departments and agencies cited in the report take steps to be certain that systems in their organizations and in Federal programs funded by them have:

- An organizational plan that segregates the duties of individuals to minimize their opportunity for misuse or misappropriation of the entity's resources.
- A system of authorization and record procedures adequate to provide effective accounting control over assets, liabilities, revenues, and expenses.
- An established system of practices to be followed for each duty and function of the organizational departments.
- An effective system of internal review. This includes an internal audit staff that has training adequate to review and evaluate computer-based system controls and that does such reviews both when systems are being designed and after they have become operational.
- Analyses of crimes to pinpoint internal control weaknesses that may have facilitated them.

Since GAO believes all agencies face similar problems, copies of the report are being sent to them for their information and use.

Departments and agencies that gave us information on computer-related crimes in their organizations were given an opportunity to comment on our report. Those that did comment agreed with our conclusions and recommendations.

CHAPTER 1

INTRODUCTION

In recent years, a new type of criminal has appeared—the computer criminal. Well-publicized crimes have demonstrated that computer-based systems are vulnerable to criminal activity, and hundreds of computer-related crimes have been detected. The dollar value of reported computer-related bank embezzlements, for example, ranged from about \$1,000 to almost \$7 million.¹

Faced with the possibility of such activity in Government, we reviewed computer-related crimes in Government organizations. Since we promulgate Federal accounting and auditing standards and work with other levels of government to help improve their standards and procedures, our objectives in this review were to:

- Determine whether computer-related crimes are occurring in Government.
- Relate methods used by computer criminals to weaknesses in controls in the systems in which they committed the crimes.
- Examine the internal audit procedures used to review the operations affected by the crimes to determine whether changes in audit procedures, standards, or guidelines are needed.
- Identify ways to help prevent and detect future crimes.

WHAT IS A COMPUTER-RELATED CRIME?

We define computer-related crimes as acts of intentionally caused losses to the Government or personal gains to individual related to the design, use, or operation of the systems in which they are committed. Computer-based data processing systems are comprised of more than the computer hardware and the programs (software) that run on them. The systems include the organizations and procedures—some manual—for preparing input to the computer and using output from it. Computer-related crimes may result from preparing false input to systems and misuse of output as well as more technically sophisticated crimes, such as altering computer programs.

We have used the terms “crimes” and “criminals” throughout this report in lay sense. Many of the examples reported have resulted in criminal convictions. However, for various reasons, some of the incidents did not result in criminal proceedings.

FEDERAL MANAGERS HAVE RESPONSIBILITY TO ESTABLISH EFFECTIVE CONTROLS

Under the Budget and Accounting Procedures Act of 1950, the head of each Government agency is required to establish and maintain

¹ A. Donn B. Parker, Susan Nycum, S. Stephen Oura., Computer Abuse, Stanford Research Institute, 1973 (NTIS Pub. No. PB231-320/AS).

systems of internal control to safeguard assets. The same legislation requires us to prescribe accounting standards, to work with agencies in developing systems, and to audit agencies to determine the adequacy of internal controls over financial operations. In addition, we are responsible for approving agencies' accounting systems when they conform to standards prescribed by the Comptroller General.

In conjunction with the Secretary of the Treasury and the Office of Management and Budget, we have developed accounting principles and standards to be observed by executive agencies. These were published in the Comptroller General's Manual for Guidance of Federal Agencies.

Section 7 of title 2 of the manual states that an accounting system is an integral part of management control and should help safeguard "all funds, property, and other resources for which the agency is responsible * * *" from "* * * misuse [and] misappropriation * * *."

Internal auditing is one of the essential tools of management, complementing other elements of management control. Using automatic data processing (ADP) as the basis for a system requires increased emphasis on review of internal controls, because computer-based systems centralize and concentrate data processing steps.

HOW INFORMATION ON CRIMES WAS GATHERED

We obtained information on 69 cases of improper use of computers from various investigative offices. These cases, which are listed in appendix I, totaled over \$2 million. They do not represent all the computer crimes involving the Federal Government since agencies do not customarily differentiate between computer-related and other crimes. Moreover, there may be a large number of crimes which have not yet been detected or reported. For example, in just one inventory system, military investigative officials estimated that only a fifth of all losses were reported and that 80 percent of all thefts may have been computer related. Our study was aimed only at those crimes already reported.

We reviewed in detail 12 of the cases representing a cross section of the types of crimes reported to date. The details of our method of examination are in chapter 7.

CHAPTER 2

THE NATURE OF GOVERNMENT COMPUTER CRIMES

A wide variety of computer-related crimes in all levels of Government has been discovered. Most have been committed by persons who possess only limited technical knowledge of computers; that is, users of ADP systems rather than persons with more technical knowledge such as programmers, operators, or analysts. Of the 69 cases in our files, at least 50 were committed by system users, not ADP personnel.

A Stanford Research Institute (SRI) report prepared for us notes that, although sophisticated computer crimes are the ones that get publicity, most criminals discovered so far used unsophisticated methods. Moreover, most committed their crimes within their own work environments.

Our review of Government cases shows results similar to those in the Stanford Research report.

WHAT KINDS OF CRIMES ARE OCCURRING?

We can best illustrate the varied types of crimes by giving some examples of cases gathered from agency records.

The majority of cases—about 62 percent—involved persons preparing fraudulent input to computer-based systems. (See chart on p. 6.) Several variations of this method have been discovered.

Supply systems are particularly vulnerable to fraudulent input. In one case, a perpetrator used a computer terminal to ascertain the location and availability of items desired by outside conspirators. Once he located those items, the perpetrator caused the system to prepare fraudulent requisitioning documents. Then he used the documents to obtain the items he wanted, took the items from the installation, and sold them to the outside parties. Although the total amount of property stolen through computerized supply systems cannot easily be determined, the value of one such theft in our case files was about \$53,000. Another loss of over \$300,000 was averted when discrepancies were discovered accidentally and the material recovered.

Many cases discovered to date in which the individuals involved prepared fraudulent input involve systems that make direct payments to individuals or businesses. These include fraudulent payroll, social welfare, and compensation transactions as well as payments for nonexistent goods and services. For example:

A Government employee who had helped automate an accounting system introduced fraudulent payment vouchers into the system. The computer could not recognize that the transactions were fraudulent and issued checks payable to fictitious companies set up by the employee and his accomplices. These checks

were sent directly to banks where the conspirators had opened accounts for the companies. The criminals then withdrew the funds from the accounts. Officials estimated the Government may have paid this employee and his accomplices \$100,000 for goods that had never been delivered.

—A supervisory clerk responsible for entering claim transactions to a computer-based social welfare system found she could introduce fictitious claims on behalf of accomplices and they would receive the benefits. She was able to process over \$90,000 in claims (authorities believe it might have been up to \$250,000) before she was discovered through an anonymous telephone tip.

Another type of act, which has occurred in several agencies, is the unauthorized use of computers by ADP personnel. An engineer who was no longer employed at a computer installation managed to continue using the equipment for his own purposes. Before he was discovered, he had used over \$4,000 worth of computer time. At another installation, a programmer used a self-initiated training program to obtain use of his agency's computer system. But instead of working on the training exercise, he was developing his own computer programs which he hoped to sell.

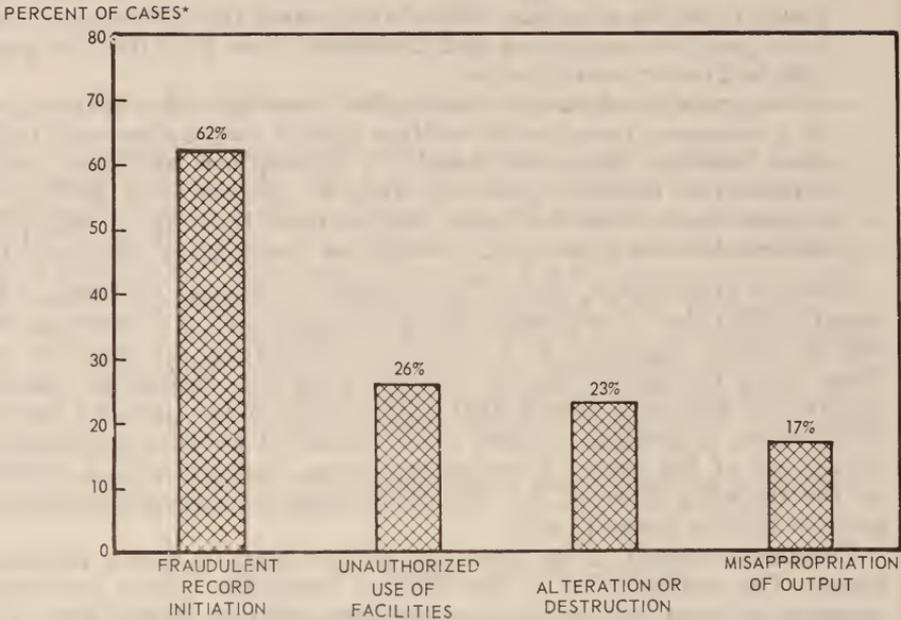
Computer-related crime does not always lead to direct monetary losses: The manager of a non-Federal computer center processing personal information was able to steal some of this data and sell it to outside parties who were not authorized to use it. Although the Government did not lose any money, the privacy of individuals whose data records were involved was violated, and this is of concern in protecting the privacy of personal information.

For convenience, we have categorized the methods used to commit known Government computer crimes.

Category 1—initiation of fraudulent records (input)

Includes such crimes as deliberately falsifying input documents or records, entering counterbalancing transactions, and falsifying claims by reuse of supporting documents previously processed.

TYPES OF COMPUTER-RELATED CRIMES IN GOVERNMENT



*PERCENTS TOTAL MORE THAN 100% BECAUSE SOME CASES APPLY TO MORE THAN ONE CATEGORY.

Category 2—unauthorized or inappropriate use of facilities and supplies

Includes developing salable programs on organizations' computers, doing commercial service-bureau-type work for outsiders on organizations' computers, using remote terminals for personal benefit, and duplicating magnetic files and selling them.

Category 3—processing alteration or destruction

Includes such crimes as sabotage or altering information recorded in the files affecting pay, promotion, or assignment and bypassing existing controls to enter unauthorized changes. These crimes could be done by operators intervening to perform unauthorized processing, resulting in gain to the operator or his accomplice, or by programmers altering computer programs.

Category 4—misappropriation of output

Includes such crimes as misappropriating returned checks and eliminating or altering notices designed to provide controls and balances.

The chart on page 6 shows the percentage of cases in our files which relate to each of the categories.

HOW DO GOVERNMENT CRIMES COMPARE TO THOSE IN THE PRIVATE SECTOR?

The Stanford Research Institute report indicates the same types of crimes occur in both the public and private sectors. However, the

cases we reviewed involve a greater proportion of financial frauds than those in the SRI files (67 percent versus 33 percent) and a smaller proportion of vandalism and unauthorized use of services (3 percent Government versus 40 percent SRI). In both sets of files, the majority of crimes were committed by systems users, but the proportion of user crimes is larger in Government.

The size of the average loss in private sector crimes is higher than in our Government cases. According to another SRI report, the average loss for each case in 144 cases since 1963 was \$450,000. The average loss of the Government cases, for which a dollar loss was applicable and was determined, was about \$44,000. (See app. I.)

We do not know why the average losses in detected Government cases are smaller than those in the private sector. But, from a security standpoint, Government systems are similar to those in private businesses. Therefore, as the SRI report to us points out, there should be equal opportunity and temptation for the perpetration of computer crimes.

WHY DO THESE CRIMES OCCUR?

In every case we reviewed in detail, the incidents were directly traceable to weaknesses in system controls. These weaknesses were the result of deficient systems designs, improper implementation of control by operating personnel, or a combination of both. Moreover, the weaknesses were in basic management controls, such as separation of duties and physical access control over facilities.

The primary reason weaknesses in system controls existed was that management failed to recognize the importance of controlling systems. This lack of emphasis affected both the way systems were designed and the extent to which operating personnel enforced controls.

Managers can use internal auditors as an important part of management control. But agencies' internal audit groups vary greatly in how they review ADP systems. Often the auditors were not aware of crimes that demonstrated weaknesses in internal control systems.

The following chapters explain the types of control weaknesses which have been exploited, the importance of management emphasis on controlling systems, and the roles played by auditors in the cases we reviewed.

CHAPTER 3

CRIMINALS EXPLOITED WEAKNESSES IN BASIC MANAGEMENT CONTROLS

System controls are designed to protect the assets of an organization. Thus, it is not surprising that, in committing their crimes, perpetrators take advantage of system control weaknesses. What may be surprising is that the weaknesses exploited are mostly basic management controls long recognized as being necessary to insure proper operations.

The characteristics of a satisfactory system of internal controls include:

1. An organizational plan that segregates duties of individuals to minimize their opportunity for misuse or misappropriation of the entity's resources.
2. A system of authorization and record procedures adequate to provide effective accounting control over assets, liabilities, revenues, and expenses.
3. An established system of practices to be followed for each duty and function of the organizational departments.
4. An effective system of internal review.

The most common weaknesses which have been exploited in our cases were in (1) separation of duties and (2) physical control over facilities and supplies. Sometimes these weaknesses are due to poorly designed systems, but in 7 of the 12 cases we reviewed in detail, controls or procedures existed but were not enforced by operating personnel.

INADEQUATE SEPARATION OF DUTIES AND POOR PHYSICAL CONTROLS ARE THE MOST COMMON WEAKNESSES

Using computers compresses activities into fewer hands. Under such circumstances, management should critically evaluate the amount of control any one individual exercises over processing steps. In 7 of the 12 cases, inadequate separation of duties was a major weakness contributing to the perpetrators' successes.

In one social benefit program, the perpetrator was a system user, a representative responsible for certifying the eligibility of benefit recipients. But he also prepared data to be put into the ADP system for controlling and issuing negotiable coupons. Although the system identified some discrepancies, no one investigated or reconciled the discrepancies. Using his position in the organization to his own advantage, he processed a series of fraudulent claims, causing coupons to be sent to accomplices not eligible to receive them. The coupons were then redeemed by accomplices. No one reviewed the validity of transactions initiated by this clerk, and he did not even have to prepare backup source documents to support the fraudulent claims.

ADP personnel also can take advantage of too much concentrated authority and responsibility. One of our cases involved the manager of a small non-Federal computer center. This person had authority to establish procedures at the center, revise those procedures at his own discretion, and circumvent established operational controls with little or no review by supervisors or system users. He used his position to sell information on private citizens to special interest groups which paid him an estimated \$48,000 for that information. As previously stated, this violated the privacy of persons whose records he sold.

Another common weakness is poor physical control of facilities and supplies. Some examples of these weaknesses include unauthorized access to computer rooms, unauthorized use of terminals, unrestricted access to computer tape files, and free access to documents authorizing transactions. Such weaknesses led directly to improprieties in 5 of the 12 cases.

ONCE DESIGNED, CONTROLS MUST BE USED

Even though a system design may include adequate controls, they are ineffective unless persons using and operating the systems are required to use the controls.

One Federal installation followed a common practice prohibiting programmers from operating computer equipment except in special circumstances and only with approval from the appropriate division chief. However, authorized computer operators allowed programmers to operate equipment on several occasions without knowing whether the programmers had proper approval to do so. Operators said they did this to help programmers test their programs, and the operators even started the equipment for them. Unfortunately, one of the programmers was using the computer to develop his own programs, which he hoped to sell commercially.

The SRI report states the most effective safeguards against most computer-related crimes discovered to date in the private sector are separation of duties and other management controls that are traditionally included in any well-designed system.

Failings in these same areas—in basic management controls—contribute to Government crimes, too. Although computer technology requires that these controls be implemented using more sophisticated techniques, they are still essential. Management should be concerned first with basic administrative controls to tighten system security.

CHAPTER 4

MANAGEMENT DOES NOT PLACE SUFFICIENT EMPHASIS ON CONTROLLING SYSTEMS

Primary responsibility for control of operations rests with top management—a legal requirement in Federal agencies as well as a tenet of sound management practice. Our review showed that managers often do not place sufficient emphasis on controlling systems, and this lack of emphasis results in poorly designed or inadequately enforced controls. This presents increased opportunities to criminals.

MANAGEMENT PLACED PRIORITY ON MAKING SYSTEMS OPERATIONAL RATHER THAN ON CONTROLLING THEM

Managers of organizations involved in many of the 12 cases we reviewed had primarily emphasized making their systems operational: control was not emphasized.

In one case involving a social compensation system, automatic data processing personnel told us their organization's processing was built around second-generation computers and had no fraud-oriented controls built in. When they converted to more modern equipment, the system was not redesigned because of pressure to get the new computers running. An employee submitted fraudulent claims to this system, and the system sent her checks totaling over \$15,000.

Another case involved a contractor ordering Government-furnished material for approved contracts directly through a Government supply system, using a remote terminal device. No controls existed to insure that the material ordered (by type or quantity) was appropriate to a given contract, and the contractor requisitioned over \$300,000 worth of material to which it was not entitled and for which it would not have paid. In designing the system, officials had emphasized speeding up the requisition process; they considered time more critical than controls that might delay delivery.

Management should give attention to controlling systems as well as to implementing them. Managers should continuously assess operations to insure a proper balance between performance of systems and control over assets.

MANAGEMENT DID NOT ASSESS POTENTIAL THREATS TO SYSTEMS

The National Bureau of Standards published in June 1974 Federal Information Processing Standards Publication 31, entitled "Guidelines for Automatic Data Processing Physical Security and Risk Management." This publication provides suggestions for managers in assessing potential threats and losses to systems in terms of both physical and data security.

A similar risk assessment concept is proposed in Federal Information Processing Standards Publication 41, "Computer Security Guidelines for Implementing the Privacy Act of 1974." This publication states the premise that the first step in improving a system's security is to analyze its security risks.

Although the importance of such analyses is now gaining recognition, most of the organizations involved in the cases we reviewed had not made such an analysis before being victimized. One agency did make a threat study after investigating a crime and, as a result, implemented several new controls.

Other agencies now are starting to analyze threats to computer systems. One example is the U.S. Army Intelligence Agency, which uses a threat model to evaluate security at ADP installations. This model describes the ADP installation being reviewed and is used by the agency's staff to ascertain potential security problems at the installation. Analyses of potential threats and losses to identify the need for and types of cost-effective controls are necessary for managers to carry out their responsibilities to control assets.

The Stanford Research Institute report points out that one of the key elements in operational security is management support. Inadequate control often can be traced to lack of management attention to the problem. In view of the crimes discovered to date and the potential for more losses, it is important that top managers recognize the need for proper security, systems controls, and supervision.

CHAPTER 5

IMPROVEMENT NEEDED IN AUDITS OF SYSTEM CONTROLS

Internal auditing is an important part of the management control function. It complements other elements of management control, and it provides independent judgment on the ways managers have carried out their responsibilities.

Our standards for Audit of Governmental Organizations, Programs, Activities, and Functions require evaluations of systems of internal control.

Proper auditing of system controls and procedures can detect weaknesses that facilitate criminal activity and can help discourage potential criminals. But Federal agencies' internal audit groups vary greatly in how they review automatic data processing systems. In 9 of the 12 cases we studied, auditors had not reviewed controls in the systems involved. To plan their work properly, audit staffs should be made aware of criminal activity which resulted from weaknesses in controls. But often they are not.

PROPER AUDITS CAN DETECT WEAKNESSES THAT LEAD TO CRIMES

The auditor's responsibility in detecting fraud is the subject of current controversy. However, adequate reviews of internal controls can and do help detect weaknesses that facilitate crimes, thus helping management prevent them. Audits or special reviews in 13 of the 69 cases in our files—about 19 percent—actually did result in the discovery of improprieties.

Auditors reviewing system controls in two of the cases identified and reported weaknesses in them. In both cases, the auditors made recommendations to correct the weaknesses, but in each case management action was inadequate. The weaknesses continued to exist, and the criminals took advantage of them.

The Stanford Research Institute report points out that auditing can be a deterrent to potential criminals. Computer criminals are typically not "professional" criminals, but persons who have encountered difficulties on a short-term basis and who commit their crimes to help them solve their problems. They experience great personal suffering when their acts are discovered. Therefore, a highly visible and active audit function could dissuade them from attempting crimes.

AUDITS OF CONTROLS HAD NOT BEEN MADE

We found wide variations in the approaches Federal agencies' internal audit staffs have taken to review ADP systems. Some auditors become involved during system development, and some do not. Use of specific audit techniques, such as test decks, retrieval packages, and

specially written computer audit programs, varies widely. Most agencies believe their audit staffs should have knowledge about various aspects of ADP—such as design, operation, and controls—but the auditors' own estimates of their abilities to address these areas show great differences.

No internal audits of system controls had been made in 5 of the 12 cases. In four other cases, investigative officials, not auditors, had reviewed specific systems controls as they related to crimes already detected. Even the one agency in which auditors' reviews had revealed system weaknesses, Federal officials responsible for the audits stated that the programs involved were so large the agency did not have the resources to make onsite inspections or followup reviews on recommendations. They stated they had to do much of their work through correspondence and meetings. They did not assure themselves management had taken appropriate action on reported deficiencies.

Although we cannot say that audits of controls would have detected or prevented all 69 incidents, such audits are recognized as an important part of good overall management control. Some agency officials told us of specific plans to review systems procedures and controls, and some had been reviewing them regularly. Others had not, and overall we found audits of controls either inadequate or ineffective.

AUDITORS SHOULD BE INFORMED OF CRIMINAL ACTIVITY INDICATING CONTROL WEAKNESSES

Information on frauds and unusual irregularities should be made available to us and to others in the agencies who may legitimately inquire into them. This is pointed out in title 7 of our Manual for Guidance of Federal Agencies. But agency internal auditors often had not been informed about computer-related crimes so they could consider their effect on audit procedures. In several of the cases we reviewed, auditors told us our inquiry was the first time they had heard of the crimes.

Some agencies' audit officials told us they did have informal cooperative procedures with investigators in their agencies. One agency, which now recognizes the need to share information, told us it is establishing formal cooperative procedures at policy levels as well as at working levels.

For internal auditors to be responsive to needs of management and the organization, they should have information necessary to develop adequate work procedures. Sharing information on criminal activity involving systems problems at various organizational levels is necessary to insure good planning of audits.

CHAPTER 6

CONCLUSIONS AND RECOMMENDATIONS

The number of computer-related crimes in Government as well as in the private sector is cause for concern about how well systems are being controlled. The dollar values of Government cases we know about are not as large as those in some crimes in private businesses, but we cannot be sure whether factors in Government systems prevent larger losses or whether we simply have not uncovered larger crimes.

It is clear the potential for computer-related crimes exists, especially since reliance on the computer is increasing. We know that weaknesses in the design and the execution of controls in automatic data processing systems make it easier to commit crimes. We have evidence that security surrounding Federal computer installations and applications is about the same as that in the private sector, and in our own reviews of Federal agencies' systems, we continue to find weaknesses in design and enforcement of controls.

Computers have added a new dimension to the potential for crimes. They can make crimes harder to detect because computer-based systems usually provide fewer written records of transactions. These systems naturally concentrate processing in fewer hands and make proper separation of duties more difficult to achieve. The concentration of asset information in easily changed form increases the potential size of each loss.

As a result of these characteristics, there should be a more systematic approach to preventing and detecting crimes in computer-based systems than was necessary for manual systems. This means better internal control and more effort to see that the system is operating as designed.

RECOMMENDATIONS

Although Government-wide standards on internal controls and on audits of internal controls have existed for several years, heads of Federal organizations need to insure that adequate controls are designed into computer-based systems serving them and that those controls are functioning properly.

We recommend that the heads of the organizations which gave us information on computer-related crimes which have occurred in their departments or agencies—the Departments of Defense (Army, Navy, and Air Force); Agriculture; the Treasury; Health, Education, and Welfare; the Interior; and the Veterans Administration—take steps to insure that systems in their organizations and in those supporting programs they fund have:

—An organizational plan that segregates the duties of individuals to minimize their opportunity for misuse or misappropriation of the entity's resources.

- A system of authorization and record procedures adequate to provide effective accounting control over assets, liabilities, revenues, and expenses.
- An established system of practices to be followed for each duty and function of the organizational element.
- An effective system of internal review. This includes an internal audit staff that has training adequate to review and evaluate computer-based system controls and that does such reviews both when systems are being designed and after they have become operational.

If crimes occur, they should be analyzed to pinpoint the internal control weaknesses that may have facilitated them. Therefore, we also recommend that analyses of such crimes be made and results provided to managers, designers, investigators, and auditors to help them strengthen their operations and procedures.

Although we are making the above recommendations to those organizations which gave us information on cases they discovered, all departments and agencies that use computers or sponsor programs in which computers are used are equally vulnerable to computer-related crimes. We are therefore sending copies of this report to other departments and agencies for their information and use; we urge them to take the steps stated above to insure the propriety of their operations.

We believe the guidance on internal controls, internal audit, and accounting methods provided in our Policy and Procedures Manual for the Guidance of Federal Agencies and in our audit standards, gives appropriate general criteria. In determining whether an agency's accounting system meets the standards for approval by the Comptroller General, we always review the internal controls designed into the system to be sure that they are sufficient. A special check is made of computer controls whenever a computer is involved.

In addition to the above matters, we are developing some more detailed guidance which we plan to distribute to departments and agencies in the near future. These will include:

- Information on various Federal internal audit groups' work in ADP systems reviews, highlighting procedures and techniques which may be useful to others.
- Audit guides for evaluating automated systems.
- Audit guides for assessing the reliability of computer-produced information.
- Our criteria for evaluating automated accounting systems' designs for approval.

We are providing copies of this report to all Federal departments and agencies to help them take appropriate steps to achieve the necessary internal control over their computer systems.

AGENCY COMMENTS

We gave departments and agencies that provided us information on computer-related crimes an opportunity to comment on our report. Each of them that did comment agreed with our conclusions and recommendations.

CHAPTER 7

SCOPE OF REVIEW

We initially requested information on discovered cases of computer-related crimes from the investigative agencies listed below. These agencies generally did not classify case files as computer related, so their responses were based on file searches and, in some instances, on personal recollections of agents or attorneys.

Using this method, we obtained background information on 74 cases. Our examination showed that 69 of these cases fit our definition of computer-related crimes. (See p. 1.)

Agencies which gave us information on cases were:

1. Department of the Army, Criminal Investigations Division Command.
2. Department of the Navy, Navy Investigative Service.
3. Department of the Air Force, Office of Special Investigations.
4. Department of Justice:
 - a. Executive Office for United States Attorneys.
 - b. Federal Bureau of Investigation.
5. Department of Agriculture, Office of Investigation.
6. Department of the Treasury, Internal Revenue Service.
7. Department of Health, Education, and Welfare, Social Security Administration.
8. Department of the Interior, Division of Investigation.
9. Veterans Administration, Investigation and Security Services.

We selected 12 representative cases to review in detail, sending staff to the sites where the incidents occurred. The cases selected included four direct payment system cases, one personnel system case, five supply system cases, and one case in which personal information derived from Federal sources was used by a non-Federal agency. In three of these cases, we were able to interview the perpetrators of the crimes.

Our work at the sites included interviews with both ADP and functional users who had knowledge of the perpetrators and of their duties. In addition, we interviewed investigative staffs at the local sites to obtain additional information on the incidents. We interviewed local audit staffs and headquarters officials to learn what audit procedures had been used in covering the operations of systems involved.

Mr. Donn B. Parker of the Stanford Research Institute, who has been studying computer abuse since 1966, prepared a report for us based on his information. His files contain over 380 cases.

APPENDIX I

APPENDIX I

CASESINCLUDED IN OUR REVIEW

<u>Description/ amount of loss</u>	<u>Method used by perpetrator</u>			
	<u>Fraudulent record initiation</u>	<u>Improper use of facilities</u>	<u>Processing alteration</u>	<u>Misappro- priation of output</u>
Fraudulent direct payments:				
1. \$ 3,680	X			
2. 250,000	X			
3. 1,120	X			
4. 28,000	X			
5. 100,000	X			
6. 25,000	X			
7. (a)	X			
8. 8,000	X		X	
9. 14,000	X			X
10. 15,480	X			X
11. 79,780	X			
12. 30,000	X			
13. 134,000	X			
14. (a)	X			
15. 16,113	X			
16. (a)	X			
17. 371	X			
18. 4,400	X			
19. 668	X			
20. 360		X	X	
21. 4,476	X	X		
22. 1,411	X			
23. 6,000			X	
24. 14,400			X	
25. (a)	X			
26. 320	X			
27. (a)	X			
Fraudulent inventory/supply actions:				
28. 53,000	X			
29. b/766	X			
30. b/11,000	X			
31. b/64,000	X			

APPENDIX I

APPENDIX I

Description/ amount of loss	Method used by perpetrator			Misappropriation of output
	Fraudulent record initiation	Improper use of facilities	Processing alteration	
32. (a)	X	X		
33. 3,800	X	X		
34. 13,000	X	X		
35. b/330,000	X	X		
36. 978	X			
37. 8,000	X			
38. 69,000			X	
39. (a)	X			
40. 29,000	X			
41. 12,740	X			
42. b/530,000	X			
43. 22,600	X			
44. 184	X		X	
45. 1,500	X			
46. 250,000	X			
47. 101				X
48. 1,293				X
49. 6,749				X
50. 358				X
51. 2,989				X
52. 3,074				X
53. 961				X
54. (a)				X
55. 2,609				X

Unauthorized altering
of personnel records:

56. (c)		X	X	
57. (c)		X	X	
58. (c)		X	X	
59. (c)		X	X	
60. (c)		X	X	
61. (c)		X	X	
62. (c)		X	X	
63. (c)	X	X	X	

Use of facilities
for personal
benefit:

64. (c)		X		X
65. 1,832		X		
66. (a)		X		
67. 4,300		X		

APPENDIX I

APPENDIX I

Description/ amount of loss	Method used by perpetrator			
	Fraudulent record initiation	Improper use of facilities	Processing alteration	Misappro- priation of output
Sabotage of operations:				
68. (a)			X	
69. (a)	--	--	<u>X</u>	--
Totals \$ <u>2,161,413</u>	<u>d/43</u>	<u>d/18</u>	<u>d/16</u>	<u>d/12</u>

Notes:

a/Loss has not been determined at the time of our review.

b/Potential loss. Crime was discovered before total loss occurred.

c/No monetary loss. Effect was of another type; e.g., invasion of privacy.

d/Total exceeds 69 since some crimes involved more than one method.

**REPORT TO THE CONGRESS BY THE COMPTROLLER
GENERAL OF THE UNITED STATES—MAY 10, 1976**

**MANAGERS NEED TO PROVIDE BETTER PROTECTION
FOR FEDERAL AUTOMATIC DATA PROCESSING FA-
CILITIES**

MULTIAGENCY

Physical security policies and practices employed at Federal data processing installations to prevent losses caused by bombings, fires, floods, frauds, thefts, embezzlements and human errors need improvement.

GAO recommends that the Office of Management and Budget direct that

- At each Federal computer installation a management official be designated as specifically responsible for automatic data processing physical security and
- He use risk management techniques when determining the protection needed.



COMPTROLLER GENERAL OF THE UNITED STATES
WASHINGTON, D.C. 20548

B-115369

To the President of the Senate and the
Speaker of the House of Representatives

This report summarizes our findings about the adequacy of physical security and risk management policies and practices employed at Federal data processing installations to prevent losses caused by bombings, fires, floods, frauds, thefts, embezzlements, and human errors.

We made our review pursuant to the Budget and Accounting Act, 1921 (31 U.S.C. 53), and the Accounting and Auditing Act of 1950 (31 U.S.C. 67).

We are sending copies of this report to the Director, Office of Management and Budget; the Secretary of Commerce; and heads of Federal departments and agencies.

A handwritten signature in cursive script, reading "Lewis B. Statts".

Comptroller General
of the United States

DIGEST

Currently the Federal Government relies on the services of about 9,000 computers in its day-to-day operations. The total value of this equipment is many billions.

The value of some of the data which is processed on these computers, such as social security records, is immeasurable. Consequently, protecting equipment and data from unauthorized or inadvertent acts of destruction, alteration or misuse is a matter of inestimable importance.

To illustrate, the National Aeronautics and Space Administration could not carry forth its space programs and the Federal Aviation Administration could not control aircraft effectively without computer assistance. Many computers are used to manage the more than half-billion transactions processed by the Social Security Administration and the four billion facts relating to the national population compiled and managed by the Bureau of the Census. Many other agencies could continue to function only at reduced levels of efficiency and effectiveness if computers were not used.

Catastrophic losses to Government-sponsored data processing installations, such as the loss of human life, irreplaceable data, and equipment, have occurred. In many of the examples cited, additional security measures were implemented subsequent to the loss.

Information on the physical security measures employed by 28 Federal data processing facilities led GAO to believe that many Federal data processing assets and much valuable data are not protected properly.

Some managers were not confident that they had the right degree of security for their facility; some have implemented sophisticated physical security measures, and others have operated with minimal security.

Less than half of the 28 installations visited had developed and put into operation contingency plans to provide for continuity of operations if a loss occurred. The impact from losses at data processing installations which did not have contingency plans could

- Interfere seriously with efficient and economical operations of Government,
- Have an immeasurable impact on individuals and organizations relying on Government data, and
- Result in costly reconstruction efforts.

Managers of Federal data processing centers have been undertaking physical security measures based on experience, subjective judgment, and advice received from managers of other installations.

In 1974 the National Bureau of Standards issued guidelines for establishing physical security measures for data processing activities.

The guidelines provide detailed suggestions for making essential security decisions. This includes use of a risk management concept where security measures are related to the value of the data and the equipment; i.e. costly measures would not be taken to protect data or equipment of relatively low value.

The National Bureau of Standards guidelines provide the suggestions needed for a strong security program. However, the guidelines, as issued, are only a reference document and there is no require-

ment that agencies must use them when determining their security needs.

To provide more security over Government automatic data processing operations at a reasonable cost, GAO recommends that the Director of the Office of Management and Budget direct that management officials be appointed at Federal installations having data processing systems and that they be assigned responsibility for automatic data processing physical security and risk management. GAO also recommends that these officials be directed to use the National Bureau of Standards guidelines when developing physical security and risk management programs.

The Office of Management and Budget agreed that there is a need for a greater awareness of threats to physical security and said that this report should serve as a strong reminder to Federal managers on the importance of security measures on the importance of security measures for automatic data processing facilities. It questioned, however, the appropriateness of directing that a separate official be named for automatic data processing security. The Office of Management and Budget believes the agency head should be responsible for determining both the security measures needed, as well as how to organize its operations to insure effective security.

GAO recognizes that an agency head is responsible for the agency's overall management and operation and this makes his day-to-day responsibilities most demanding. Since data processing operations are so important to the well-being of most agencies, GAO believes that this responsibility should be delegated to a management official who is knowledgeable in agency missions, as well as in data processing and security matters.

CHAPTER 1

INTRODUCTION

Computers have become an integral part of the Government process by performing many of the operations and applications that, in the past, were not done at all or were done manually. Some agencies would find it impractical, if not impossible, to accomplish their missions without computers. To illustrate, the National Aeronautics and Space Administration could not carry forth its space programs and the Federal Aviation Administration could not control aircraft effectively without computer assistance. Many computers are used to manage the more than half billion transactions annually processed by the Social Security Administration and the four billion facts relating to the national population compiled and managed by the Bureau of the Census. Many other agencies could continue to function only at reduced levels of efficiency and effectiveness if computers were ~~not~~ used.

The Federal Government is the largest user of computers. In addition to the cost of acquiring and operating computers, vast sums are expended for:

- Software programs to make computers run,
- Communication links between computer components,
- Buildings and associated expenses to house data processing operations, and
- Processing and storing data.

It has been estimated that over \$10 billion is spent annually to acquire equipment and to operate Federal data processing activities.

Of more importance than the concern over the monetary value of these assets is the centralization and concentration of data in computerized environments which increases the potential for major losses or misuses that could

- Affect the successful accomplishment of agency mission and goals,
- Have an impact on those who rely on valuable or irreplaceable Government records, or
- Harm individuals on whom information is maintained.

There is, therefore, a need to protect these assets and to provide for continuity of operations should a catastrophe occur.

SOME DEFINITIONS

Data processing security is a means of safeguarding hardware, software, data, personnel, and facilities against loss from accidental or intentional disclosure of data, modification of data, destruction of assets, or both. Physical security includes the protection of equipment, personnel, facilities, and data involved with computerized processing; and provides for recovery in case of damage or loss. Such protection

is provided by various means, including restrictive access and administrative controls for data processing activities, as well as applying other measures required for protection of structures, equipment and data against accidents, fires, floods, bombings, and other hazards.

Perfect security is generally regarded as unattainable; therefore, the aim of a good physical security system should be to reduce the probability of loss to an acceptable low level at reasonable cost and to insure adequate recovery in case of loss. Many articles and publications have been written lately which say that a good security program can only be achieved by having high level management responsible for the automatic data processing (ADP) security program and using some of systematic approach when making physical security decisions.

There are many many ways and approaches to help management make ADP security decisions. One approach advocated by experts, which we believe to be a good approach, involves a concept of risk management. This concept is an element of managerial science that is concerned with identification, measurement and control of uncertain events. It:

- Analyzes the risks involved,
- Summarizes risk findings for management use,
- Involves high level management in the decisionmaking process,
- Implements the most cost effective security practices to control unacceptable risks, and
- Reevaluates periodically the potential impacts from threats to asset values and mission accomplishments and decides on new or existing practices to handle the risks.

(For a full explanation of this concept, see appendix I.)

Proper physical security, as discussed in this report, is a prerequisite to achieving adequate data security and privacy protection. To have safe and reliable Government data, it is necessary to have a good data security program for protection against accidental or intentional destruction, disclosure or modification of data in a system. In a computerized system where large quantities of data can be centrally accumulated, stored, and integrated with data from other systems, appropriate administrative, technical and physical safeguards are more necessary than in a manual system.

RESPONSIBILITY FOR SECURITY

Public Law 89-306 (Brooks Act) was passed in October 1965 and provides for the economic and efficient purchase, lease, maintenance, operation, and utilization of ADP equipment. The General Services Administration (GSA) is responsible for the economic and efficient acquisition, use, and maintenance of ADP equipment; the Office of Management and Budget (OMB) is responsible for policy and fiscal control aspects of ADP management. The law also provides for the Department of Commerce to be responsible for developing technical standards and providing technical advisory services to Federal agencies.

In turn, heads of departments and agencies are authorized by Public Law 89-554 to prescribe regulations for the custody and preservation of their records, papers, and property. The Privacy Act of 1974, Public Law 93-579, requires, among other things, that each agency

maintaining a system of records provide appropriate safeguards to insure the security of its data.

SCOPE OF STUDY

Our study covered Government-wide policies and practices used for determining physical security requirements at Federal data processing installations. More specifically, we examined:

- Policies and procedures established by OMB and GSA regarding automatic data processing systems.
- Security techniques employed at 28 data processing installations by the Departments of the Army; Navy; Air Force; Agriculture; Transportation; State; and Health, Education, and Welfare and the Veterans' Administration.
- Types of data processing security used at selected Government contractors, universities, private companies, a bank, and a local government.
- Types of security problems experienced at 23 additional Federal data processing installations.

Major areas of security covered during our visits included steps taken by management to guard against threats of modification or destruction to the physical plant, personnel, computer hardware and software, and to the data being processed or stored by the computerized systems. We developed and used a questionnaire as an audit guideline for these visits.

A detailed compilation of data from the questionnaires is shown in appendix II. This material represents those areas of automatic data processing security that applied to each installation visited and that could be quantified for analyses.

CHAPTER 2

SECURITY AT FACILITIES VISITED WAS INADEQUATE

To obtain information on the effectiveness of procedures employed by Federal agencies, we visited 18 data processing installations within the continental United States and 10 installations overseas and observed the protection procedures for equipment and valuable data.

We found a number of conditions at these 28 installations which led us to believe that physical security was not adequate and that action should be taken to protect against losses. Some of the conditions we found which we believe provided insufficient protection to data processing equipment and data follow.

Conditions found ¹	Locations within the continental United States	Locations overseas
Fire hazards:		
Combustible paper supplies and/or magnetic tape files were stored in computer rooms which expose systems to losses from fire.....	10	4
Computers were in use in areas with only portable fire extinguishers available.....	3	1
Computers were in operation in room with no portable fire extinguishers available.....	12	4
Computers were in use above raised flooring without periodically cleaning below such flooring, which is a fire potential.....	2	4
Computers were in operation in rooms where master electrical power shutdown controls were not easily accessible at exit points.....	10	2
Flood hazards:		
Computers were in operation in areas where overhead water or steam pipes (excluding sprinkler systems) existed with inadequate provision for drainage.....	2	3
Computers were used in basements below ground level which exposes systems to potential flooding conditions.....	7	5
Susceptible to sabotage:		
Vendor service personnel were not supervised while on premises.....	5	3
In-house service personnel not controlled while in computer areas.....	3	2
Computer location was possible target for vandals.....	3	2
Susceptible to theft or misuse: Remotely accessed computer systems were in operation without software to detect improper or erroneous attempts to use the computers or data files involved.....		
Lack of contingency planning: Computerized systems were in operation without formal contingency plans to insure continuity of operations if a security event occurred.....	8	6

¹ Details supporting these and other observations relating to the lack of physical security measures are shown in appendix II.

Although the above hazardous conditions existed at sites visited, the installations had not necessarily experienced an adverse effect or loss from the lack of good physical security measures. Weaknesses, such as those noted above, however, can lead to serious consequences. We supplemented our visits by contacting 23 other Federal data processing installations within the continental United States—some of which we knew have had physical security problems—to identify impacts or effects from security weaknesses.

Of the 23 installations contacted 9 have experienced physical damages from conditions, such as attempted sabotage, fires, and floods, since January 1970. Some of the losses experienced by these and other installations are shown below to emphasize the devastating effects fire, flood, and sabotage, can have upon data processing facilities.

FIRE

Fires can cause minimal or catastrophic losses. The extent of the loss generally depends upon factors such as size and location of the fire, extent and type of fire protective devices at an installation, and the type of contingency plan available if a fire should occur.

A classic example of fire loss is the 1959 fire at the Pentagon, which destroyed three complete computer systems valued at \$6.5 million. The fire started in a vault containing stored paper and magnetic tape and spread throughout the computer center. When the fire occurred employees were unable to reach the switch to turn off the electrical power for the computer systems which created a hazardous situation for firefighting efforts.

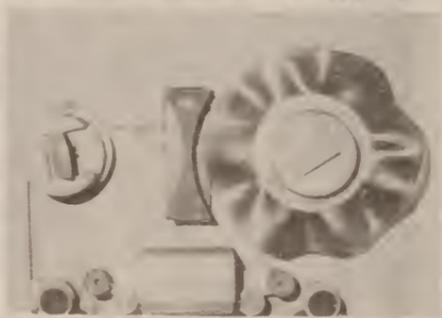
We did not attempt to relate the hazardous fire conditions we found at the 14 locations noted on page 5 to the hazardous fire condition that caused the Pentagon fire. However, we do believe that the Pentagon fire clearly illustrates what could be lost by fire at the 14 locations which had combustible paper or magnetic tape stored in computer rooms. Also, if a fire did occur at the 6 locations noted in our study where master electrical power shutdown controls were not easily accessible, the employees at the 6 locations, just like the employees in the Pentagon fire, would be unable to shut off electrical power for the computer systems.

While on major fire to Government ADP facilities has occurred lately, commercial installations have not been so lucky. For example, there was a much publicized commercial fire in 1972 which caused a \$1 million loss at International Business Machines Corporation, Hawthorne, New York.



VIEW OF PENTAGON COMPUTER FACILITY DAMAGE AFTER FIRE

(Courtesy of Department of Air Force)



VIEW OF DAMAGE DONE TO COMMERCIAL COMPUTER FACILITY
(Courtesy of International Business Machines Corporation)



VIEW OF ASHEN RECORDS AND SHELIVING
(Courtesy of General Services Administration)



**VIEW OF BUILDING CRUSHED BY COLLAPSED ROOF
AFTER ST. LOUIS FIRE**

(Courtesy of General Services Administration)

Another example of a catastrophic loss caused by fire to a Government facility, although computer records were not directly involved, was the fire at the Military Personnel Records Center in St. Louis, Missouri, in July 1973. Sections of the building housing these records were not equipped with sprinkler systems, smoke detectors or fire walls. Although the fire did major damage to paper and not computerized records it nevertheless illustrates how devastating the loss of irreplaceable documents and records can be. Since such records are being put on computers more and more the problem increasingly becomes a computer security problem.

The records center has been the repository for about 52 million records on military personnel actions since 1912. The sixth floor, where the fire started, contained about 22 million military personnel files or jackets. About 16.8 million of these records were lost.

Painstaking work is necessary to reconstruct the lost records and some may never be replaced.

Of the 18 locations we visited in the United States, 3 had only portable fire extinguishers available for firefighting protection. Also, one overseas location did not even have any fire extinguishers available for firefighting operations.

FLOOD

Since water can cause serious damage to computer records it must be guarded against as carefully as fire. Flooding has been one of the more common causes of damage to computer centers, and has resulted from sources such as storms, broken water or steam pipes, and water used in fighting fires. One case in our sample where flooding caused extended water damage was at the U.S. Postal Services ADP Center, Wilkes Barre, Pennsylvania, in 1972.

On Saturday, June 24, 1972, water from the Susquehanna River inundated all of downtown Wilkes-Barre and filled the basement of the Post Office Building. Water continued rising until about 6 inches of it were on the computer room floor. About \$7.5 million worth of Government computer equipment is located on raised flooring on the first floor. Had the water risen just an inch or so more it would have ruined almost all of the computer equipment.



VIEW OF FLOOD WATERS ON SOUTH MAIN STREET, WILKES-BARRE, PENNSYLVANIA. POSTAL ADP CENTER IS LOCATED IN THE WHITE BUILDING ON THE LEFT.

(Courtesy of Bell Telephone Company)



**FRONT VIEW OF WILKES-BARRE POSTAL
ADP CENTER ON SOUTH MAIN STREET.**

(Courtesy of U.S. Postal Service)



**SIDE VIEW OF WILKES-BARRE POSTAL
ADP CENTER.**

(Courtesy of U.S. Postal Service)

However, extensive damage was done to the building, communication lines and equipment, backup power supply, and all data processing supplies stored in the basement. Cleanup procedures required to place the data processing facility back in operation involved.

- Replacing all communication equipment and computer supplies;
- Drying out and cleaning computer equipment;
- Making extended building repairs, and
- Removing over 90 dump-truck loads of silt and debris from the building.

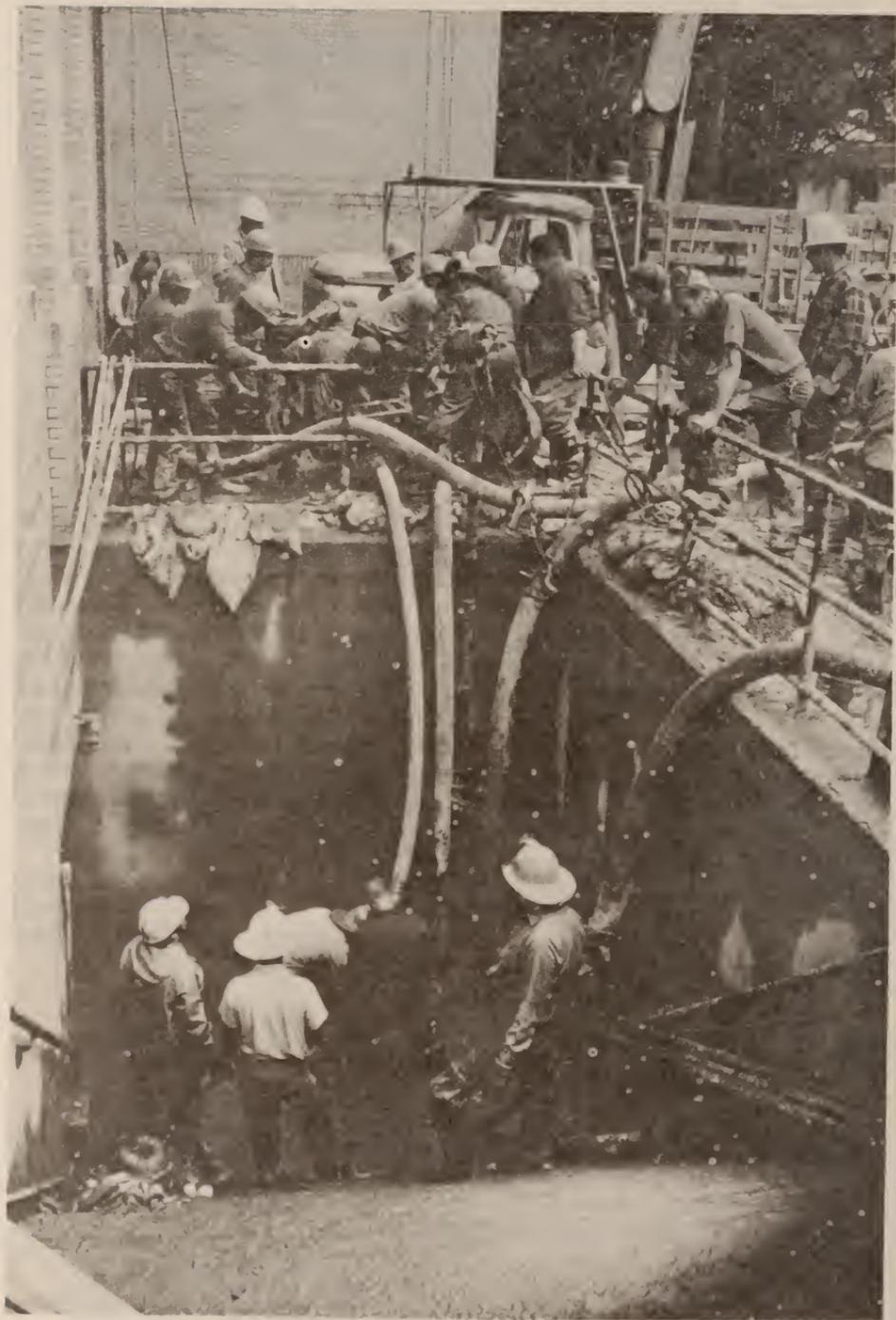
Water also was responsible for much of the damage in the Pentagon bomb incident in May 1972. In this case the computer facility was flooded from broken overhead water pipes.

During our study we identified 10 locations where computers were operating where overhead water pipes existed without adequate provisions for drainage. Also, two locations were identified where computers were operating in basements which were below ground level.

SABOTAGE

Sabotage is another problem with which many Government agencies must be concerned. For instance, on August 24, 1970, a bomb exploded outside the Sterling Hall Building at the University of Wisconsin. This building housed the Army Mathematics Research Center and other federally funded research activities. One employee was killed and three others were injured from this incident. This explosion damaged 25 buildings at the university, and resulted in a total loss of about \$2.4 million for buildings and equipment. Computers at the Army Mathematics Research Center were damaged, and some programming efforts and 20 years' accumulated data was destroyed. It has been estimated that this research data represented over 1.3 million staff hours of effort which we calculate to represent an investment of about \$16 million.

Because of this incident, the university strengthened its physical security measures by increasing the number of security guards and the activities of security patrols by adding a bomb squad and by placing greater restrictions on access to campus buildings.



**VIEW OF CLEAN-UP OPERATIONS ON SOUTH MAIN STREET,
WILKES-BARRE, PA., AFTER FLOOD**

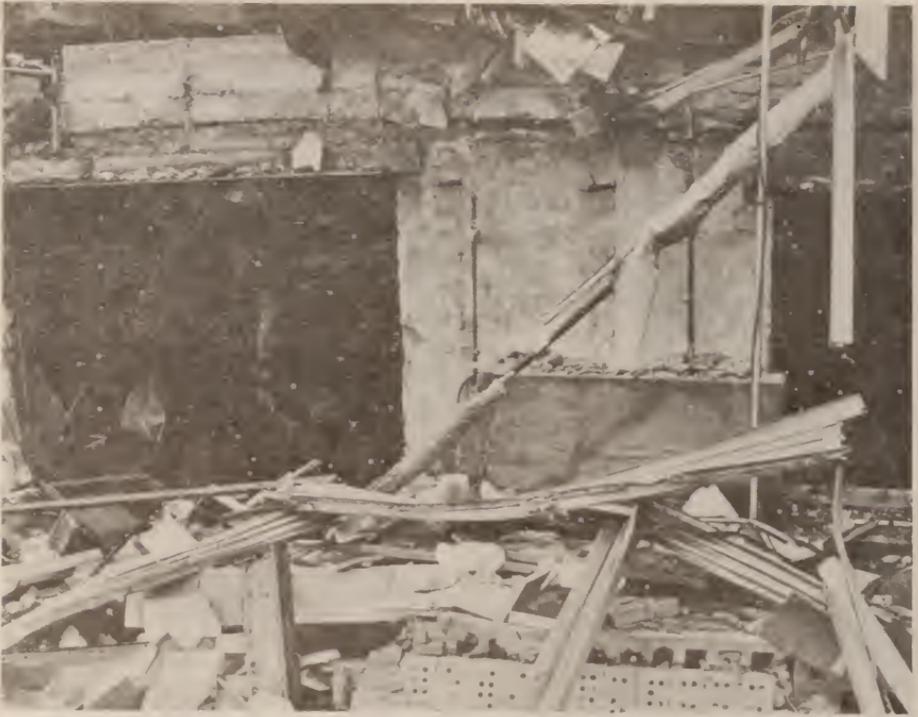
(Courtesy of Bell Telephone Company)



**VIEW OF DAMAGE DONE TO COMPUTER BUILDING BY BOMB EXPLOSION
OUTSIDE THE ARMY MATHEMATICS RESEARCH CENTER**



**CLOSE-UP VIEW OF DAMAGE DONE TO EQUIPMENT AND BUILDING BY BOMB
EXPLOSION AT ARMY MATHEMATICS RESEARCH CENTER**



CLOSE-UP VIEW OF DAMAGE DONE TO EQUIPMENT AND BUILDING BY BOMB EXPLOSION
AT ARMY MATHEMATICS RESEARCH CENTER

During May 1972 a bomb exploded on the fourth floor of the Pentagon above the computer facility and caused extensive damage. The computer facility was flooded from broken water pipes and parts of it were inoperable for about 29 hours. (See picture on p. 20.) In addition to cleanup costs, a \$21,900 removable disk storage unit had to be replaced because of this incident. The director of data automation subsequently requested that a suitable means be developed for diverting any future overhead water flow away from the computer area.

During our study we identified locations which were susceptible to sabotage (see p. 6) by not supervising service personnel while on the premises or in the computer areas. Three computer locations were also possible targets for vandals.

Attempts at sabotage of ADP activities have also been made by employees within data processing centers. For example, there were four attempts to sabotage computer operations at Wright-Patterson Air Force Base during a 6-month period ending November 15, 1974, by using magnets, loosening wires on the computer mainframe, and gouging equipment with a sharp tool. Although the financial loss from these attempts was relatively small, the local management reacted by adding controls to limit access to the computer facility and also to limit personnel traffic to authorized areas within the computer installation.

THEFT OR MISUSE

Computerized systems are also vulnerable to theft or misuse by wrongdoers. We noted numerous cases of publicized thefts or misuses involving

- Data or assets;
- Financial frauds;
- Embezzlements; and
- Mistakes made by computer employees.

Industry literature indicates thefts or misuses of computer systems are increasing at an alarming rate.

One case we noted during our study involved theft of Government funds at Kelly Air Force Base, San Antonio, Texas. The Government paid approximately \$100,000 to bogus fuel companies for aircraft fuel never delivered to the Air Force. The bogus fuel companies were established by a dishonest Government employee working at the air base. This employee had indepth knowledge of the computerized fuel accounting system which he helped develop and install. An investigation of this matter was initiated when a bank contacted the Air Force regarding suspicious banking transactions involving Government checks. The employee was later arrested and sentenced to 10 years in jail for theft of Government funds.



VIEW OF PENTAGON COMPUTER EQUIPMENT AFTER BOMB EXPLOSION
IN REST ROOM ABOVE THE COMPUTER FACILITY. PLASTIC WAS USED TO
PROTECT THE EQUIPMENT FROM DRIPPING WATER.

(Courtesy of Department of Air Force)

Other studies of theft and misuse of data processing operations have been identified within the Federal Government and private sectors. Noteworthy were March 1973 studies by the Stanford Research Institute on "Threats to Computer Systems" and a November 1973 study on "Computer Abuse." Each study catalogued over 100 data processing security incidents within and outside the Federal Government that

were identified from sundry sources. The study on "Threats to Computer Systems" also recognized the problem of identifying and solidifying security events at data processing installations and emphasized that a timelag phenomenon occurs in identifying or reporting security events.

We did not attempt to determine which locations were vulnerable to theft or misuse by Government employees at the 28 locations we visited. However, we did identify five locations where computer systems were in operation without security procedures to detect improper or erroneous attempts to use the computer or data files involved.

POWER FLUCTUATIONS

Unexpected surges or interruptions of electrical power can cause serious damages to data and computer equipment. In a computer operation which processes one job at a time, computer instructions can store data during different job stages, thus providing a limited degree of protection for possible data distortions caused by power fluctuations. The need for some form of power support or backup capability becomes more apparent with on line or real time computer systems because of the number of jobs or the mix of jobs being processed at any point of time. These types of computer systems become more vulnerable to losses caused by power fluctuations.

The computer center at the National Institutes of Health, Bethesda, Maryland, has experienced many computer system failures which have been attributed directly to fluctuations of electrical power. Officials of the computer center estimate that they lost a minimum of \$500,000 annually from electrical power fluctuations. During a 5-week period, the computer center experienced 6 major electrical power fluctuations which caused 15 computer system failures. These failures resulted in destruction of data for 375 batch processing jobs and for 2,250 remote terminal users. Moreover, these power fluctuations caused replacement of electronics costing over \$94,000 in various components of the computer systems.

Our study showed that 4 out of the 23 data processing installations contacted have experienced problems caused by electrical power fluctuations and interruptions.

There are several alternative solutions to problems related to electrical power requirements. Some installations may be located in areas where they can change sources of power supply or use secondary sources of electrical power as backup; others may need to install electrical generating plants or uninterruptible power supply systems.

CONTINGENCY PLANNING

We found that only 13 of the 28 (less than 50 percent) of the Federal installations visited during our study had written contingency plans to insure continuity of data processing operations if a loss should occur. Contingency planning is nothing more than developing a formalized plan of action to be taken in the event of work stoppage,

physical damage, or when a loss occurs. Such plans are generally developed to cover minor disruptions as well as catastrophic events. A typical plan might include:

- Evacuating people;
- Locking up files and facilities;
- Turning off power; and
- Making provisions for backup capabilities.

One case in our sample where losses did occur was at the Postal Service ADP Center, Wilkes-Barre, Pennsylvania. However, these losses were not catastrophic because the Postal Service had a contingency operating plan to minimize losses and continue operation.

This post office is an important cog in the postal data processing operation which services about 200,000 postal employees in 67 post offices in the Eastern and Southwestern areas of the United States. The office collected data on time and attendance for Postal Service employee payrolls, maintained labor distribution information, and gathered data on mail volume.

Although the flood occurred at the end of a pay period, the office was able to continue with its data processing function at a backup site. The workload and payroll targets were met with a minimum number of problems and the facility was back in operation in a little over 2 weeks. Some contingency procedures used during the flood were

- Removing master and other important tape files needed to continue operations to the backup facility when the water was inundating the ADP facility,
- Making provisions for processing the most critical ADP operations at the backup facility, and
- Taking necessary protection procedures to guard against flood damage when the water was rising.

The fire loss at the St. Louis Records Center is an example of what can happen when contingency plans are not made. About 16.8 million master military personnel records were lost in the 1973 St. Louis fire.

This installation's mission is to maintain these official Government records and to respond to inquiries made by the Congress, other Government agencies, and the taxpayer. This mission will now be hampered for some time because the lost records—some of which may be irreplaceable—must be reconstructed to satisfy inquiries, which is a costly and time-consuming process.

While it is unreasonable to expect that there would be backup for every original record in the manual files, it is reasonable to assume that some sort of contingency planning should have been done to insure continuity of operations when a loss has occurred. Agency officials told us that a contingency plan was formulated after the fire happened.

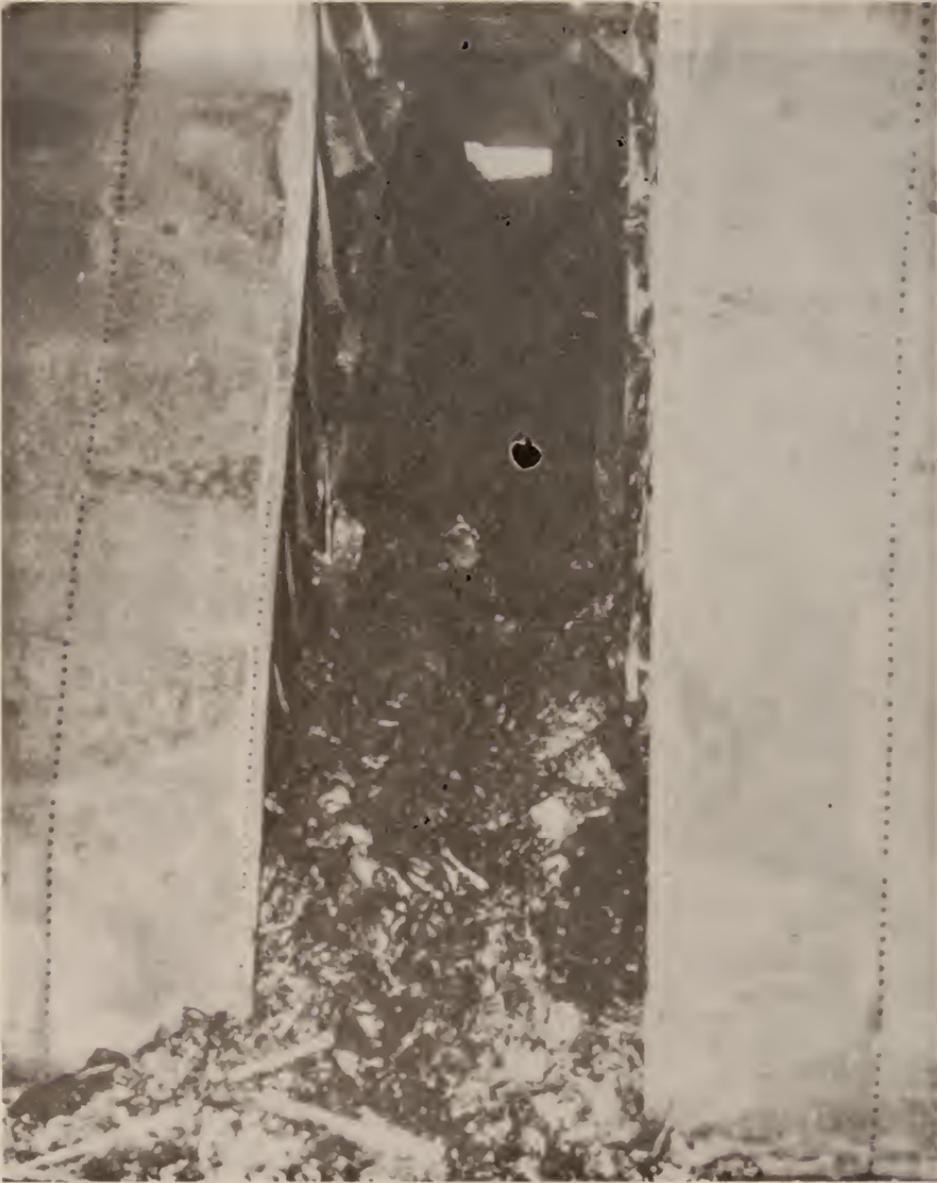
It is important to note that contingency planning and backup capabilities received a relatively low degree of concern at the Government installation we visited while the potential loss impact on individuals and organizations requiring data from computerized records was growing. Many catastrophic problems can now be caused by security losses to computer facilities.

Such problems could possibly occur at Government installations without proper security and the development and implementation of sound contingency plans for data processing activities. We hope the



**VIEW OF RECORDS DESTROYED IN ST. LOUIS FIRE.
RECONSTRUCTION WILL BE COSTLY AND TIME
CONSUMING DUE TO THE LACK OF CONTINGENCY PLANS.**

(Courtesy of General Services Administration)



VIEW OF MORE RECORDS DESTROYED IN ST. LOUIS FIRE. SOME OF THESE RECORDS MAY NEVER BY REPLACED

(Courtesy of General Services Administration)

14 locations we visited which had no contingency plans to insure continuity of operations if a security event happened (see p. 6) will recognize their errors and develop contingency plans before a loss occurs and a plan is needed.

Other types of physical losses have occurred at Federal data processing installations. In some cases the losses were small; in other cases, they were costly and disruptive. The losses or damages were caused by earthquakes, windstorms, air conditioning failures, fires, and floods. Generally, the determining factors as to the extent of the loss—whether small or catastrophic—have a direct relationship to the intensity of the security event and to the amount of protection provided by the physical security program in use by the Federal agency.

CHAPTER 3

FEDERAL DATA PROCESSING SECURITY PRACTICES

In our visits to 28 Federal installations we found that there was great diversity in the security practices employed. These practices ranged from minimal physical protection given to computers operated in an unguarded warehouse not designed for computers to very complex security measures for certain data processing centers. For the most part, Federal agency security practices have been based on:

- Data processing managers' reactions to losses that have occurred.
- Information gathered from reading technical publications or attending conferences or meetings.
- Suggestions made by agency policies such as Department of Defense Security Manual 5200.28-M.
- Recommendations made by computer manufacturers.

We found that the responsibility for data processing security was usually left to local managers of computer centers even though the data processing assets and activities involved all facets of the organizations. Security measures were usually installed by managers of data processing installations with little or no study or evaluation to determine if such devices provided the proper level of protection needed. Some installation managers were not sure whether or not their installations were over- or under-secured.

GOVERNMENT-WIDE GUIDANCE

During 1974, while we were visiting Federal installations, NBS issued Federal Information Processing Standard Publication 31, titled "Guidelines for Automatic Data Processing Physical Security and Risk Management." These guidelines should go a long way in aiding Federal officials in making and justifying essential security decisions. The guidelines were not available to those installations visited during the early days of our study. For this reason, the installations visited usually told us that there was no Government-wide guidance available for their use in the security area. (See app. IV for summary.)

It was too early to evaluate the effect of these new guidelines on Federal agencies security practices. However, we did study and review these guidelines and can say that they cover in detail numerous subjects for use by Federal organizations in structuring physical security programs for their ADP facilities. The publication discusses security analysis, natural disasters, supporting utilities, system reliability, procedural measures and controls, offsite facilities, contingency plans, security awareness, and security audit.

- We don't believe these guidelines adequately covered
- Where responsibility for physical security should be assigned; and
 - When and where the guidelines should be used.

RESPONSIBILITY FOR PHYSICAL SECURITY

The NBS publication is intended to provide guidance for *planning* a security program and therefore is directed to the security planner(s). It suggests procedures for developing and implementing a physical security program by analyzing risks, reducing exposures to losses, planning for contingencies, training personnel, and reviewing and adjusting the program.

The NBS publication does not direct much attention to the day-to-day job of seeing that the security program is properly maintained and does not specify where that responsibility should be in the organization.

Recognized experts believe that security is too important to be considered merely one of several operating functions assigned to data processing managers. Generally, data being processed originates and ends outside the data processing facility; thus there is an overall valid concern for the proper level of security over this valuable facility.

In our opinion, the responsibility for physical security needs to be assigned to a management level official of the organization who is not operationally responsible for the data processing facility. Such an individual should

- Be sufficiently knowledgeable of the operations and programs of the agency to understand the value of data and data processing facilities;
- Be sufficiently high in the organization to see the potential adverse effect losses of data processing facilities could have on the mission of the agency;
- Have the necessary authority and responsibility to establish policy and to manage all aspects of the security program; and
- Be knowledgeable of new technology for ADP security.

GUIDELINES SHOULD APPLY TO ALL FEDERAL INSTALLATIONS

The Bureau's guidelines are directed toward *new* automatic data processing systems being developed or improvements being made to existing systems. There is no requirement for applying the guidelines to all existing data processing operations.

Since December 31, 1975, the Federal Government has been using about 9,000 computers in its day-to-day operations. Because of the security events that have occurred, we believe that Federal managers need to develop a physical security and risk management program which will implement the most cost-effective security practices at existing as well as as new data processing activities.

The guidelines concentrate primarily on physical security measures for protecting equipment, personnel, and data at the computer site. Very little mention is made of the data processing activities that can be performed outside the computer center. For example, activities such as data collection, data preparation, and distribution of output to end users are important functions in a data processing operation which, in many instances, are performed outside the computer center. The guidelines fail to adequately cover these important areas and need to be strengthened to insure that adequate protection is provided.

CHAPTER 4

CONCLUSIONS, AGENCY COMMENTS, AND OUR EVALUATION AND RECOMMENDATIONS

CONCLUSIONS

Although perfect security is generally regarded as unattainable, we believe that there is a need for a high degree of insurance that data processing assets and valuable data are properly protected and that there are contingency plans to insure continuity of operations if a loss should occur. Adequate protection is needed because of the:

- Substantial investments in data processing assets and data.
- Value of data processing assets to the successful accomplishment of agency mission or goals.
- Potential for loss of irreplaceable Government records and its impact on those who rely on such records.
- Federal laws requiring that data processing assets be protected from theft, alteration, destruction or misuse.

Our study showed that computer security practices in the Federal Government have not provided the necessary insurance that data processing assets are properly protected.

We attribute the poor security measures to a general lack of concern for a comprehensive plan to provide effective security at a reasonable cost. As discussed in chapter 3, NBS in 1974 published physical security and risk management guidelines for Federal agencies when planning security measures for new or improved data processing installations. However, no policy statement has been issued by OMB regarding the application and use of the guidelines.

The NBS guidelines include details on how to protect against such threats as loss from fire, flood, sabotage, and theft, and how to decide what measures to apply in what circumstances. They also advocate a concept of risk management; that is, making a formalized assessment of the resources to be protected versus the cost to protect them and whether the cost involved is worth it.

We believe that the NBS guidelines as modified by our suggestions will provide the necessary means to structure a sound program and could go a long way in improving the conditions we found.

However, use of the NBS guidelines is not mandatory and they apply only to new installations or those which are improving their computer systems. Moreover, the guidelines do not and could not be expected to assign responsibility for this function to an appropriate management official.

AGENCY COMMENTS AND OUR EVALUATION

Comments were obtained from six Federal agencies (see app. III) on our proposals to strengthen physical security over computer systems. We proposed that the Director of OMB issue policy directing that

—Specific assignments of responsibility for physical security of ADP systems be made at each Federal installation using computer systems and

—Responsible officials use the NBS guidelines when developing physical security and risk management programs.

The Department of Health, Education, and Welfare, the Department of Transportation, and the U.S. Postal Service agreed with all our proposals. In fact, the Department of Health, Education, and Welfare and the Postal Service already have issued agency ADP security policies as we recommended in this report.

Other comments received generally concurred with our observations that improvement is needed in the physical security area; however, they differed on ways to correct or improve on the conditions found. Following is a summary of the comments.

Proposal that a management official be appointed

The Assistant Secretary of Defense and three other agencies agreed with our first proposal and suggested appointing a management official who is highly knowledgeable in ADP and security matters as well as being independent from the direct management of the ADP facility for this purpose.

The Assistant Secretary for Science and Technology, Department of Commerce, however, did not agree with our proposal and suggested that the ADP security responsibility be assigned to two different functional areas—the data processing department and the internal audit group. She suggested that the ADP organization should determine the security requirements while the audit functions should review the adequacy of the security safeguards and procedures.

The Director of OMB also questioned the proposal that a separate management official should be appointed and held responsible for ADP physical security. He said that the agency head is already responsible for protecting agency installations and that he should establish whatever safeguards are appropriate.

Our views

We recognize that an agency head is responsible for its overall management and operation and this makes his day-to-day responsibilities most demanding. For this reason, we believe that he cannot spend much time on determining what measures are necessary as well as how to organize an effective security program. Since ADP is an important issue to the well-being of most agencies, we believe that the agency head should delegate this responsibility to a management official, if one has not been designated, who is knowledgeable in agency missions or goals as well as in data processing and security matters.

Also, we know that different circumstances exist at Federal agencies and that there are different organizational structures to satisfy security responsibilities. For example, at some agencies one person or a

small staff is responsible while at other agencies a whole network of people may be required to handle the security requirements at the various installations which the agency maintains. For these reasons, it is difficult to prescribe the ideal organizational structure that would be needed at each agency to handle ADP security responsibilities. However, we do know that as a minimum a responsible management official should be assigned this responsibility at each computer installation and that he determine the proper levels of security needed under the existing circumstances.

As to the Department of Commerce comments we agree that the internal audit functions should review agency ADP security practices and procedures. However, we do not believe that the ADP organization should have the sole responsibility for determining what security practice and procedures are needed. ADP security is too important to be considered as one of several operating functions assigned to the ADP organization. At most agencies, computers are considered to be the single most important tool for management; and the data they process involves almost all facets of the organization. For these reasons, we believe that establishing and managing ADP security requires time and attention of an independent management official who has the knowledge, responsibility and authority to insure that ADP activities are properly safeguarded at reasonable costs.

Proposal that OMB issue policy instructions regarding use of guidelines.

The Director of OMB questions whether it is necessary at this time for OMB to issue any further policy directives regarding the use of the NBS guidelines. He believes that it would be more appropriate for us to direct our recommendations to improvements needed in these guidelines and to the conditions found at the installations visited.

Public Law 89-306 assigns the Government-wide policy and oversight responsibilities for ADP management to OMB while Commerce is responsible for ADP technical standards. Current Government-wide ADP policies do not adequately cover ways or concepts to protect this annual multibillion dollar activity which permeates most facets of Government operations. According to the Director of OMB, this law and Executive Order 11717, dated May 9, 1973, gives NBS the responsibility and authority to develop, coordinate, and issue appropriate uniform ADP technical standards. Had NBS issued ADP security technical standards, we would have addressed our recommendation, relative to policy directives and their use, to NBS. The NBS, guidelines, however, were issued as a reference document—not as an ADP technical standard.

The Assistant Secretary for Science and Technology, Department of Commerce, agreed to consider our suggested changes in the next edition of the guidelines. In this regard, the Assistant Secretary of Defense also voiced concern about the mandatory aspect of our recommendation. It is his view that the guidelines need further refinement before becoming a mandatory standard.

Our views

We agree that the guidelines are still in the developing stages and must be refined further. However, unless the agencies use the guidelines it will be difficult to gain the experience needed to improve them.

Moreover, the NBS guidelines are not a rigid, inflexible set of rules. They instead provide matters to be considered in arriving at an intelligent, cost-effective approach to matching risk against severity of possible loss. They are meant to be applied selectively. We believe they are a good vehicle to initiate Federal agencies in the use of sound physical security practices and risk management advocated in our report. Finally, we believe that the importance of good security for ADP's facilities outweighs any further delay for achieving more perfect guidelines.

In summary, our review showed that responsibility was not clearly fixed at installations we visited as to who should be held responsible for ADP security and what safeguards were needed to adequately protect their ADP facilities against security threats. Comments received on this report from some of the agencies showed that this confusion still exists. Without a strong Government-wide policy requiring a systematical management approach for protecting ADP assets at reasonable costs, managers of data processing installations, we believe, could continue the practices observed in this report which can result in installations being over- or under-secured.

RECOMMENDATIONS

We recommend that, in order to provide more physical security over Government ADP operations at a reasonable cost, the Director of OMB issue policy directing that:

- Management officials be appointed at Federal installations having data processing systems and that they are assigned responsibility for ADP physical security and risk management. Such officials should be aware of the impact of ADP operations on the organizations' mission or goals and the importance of the data and records to U.S. citizens and the Federal Government. Also, the official should be knowledgeable in data processing and security matters.
- These officials use the NBS guidelines when developing and implementing physical security and risk management program.

Also, since we believe that ADP security is an important matter, we are sending copies of this report to each Federal agency head for their information and use.

A CONCEPT FOR USEINMAKING SECURITY DECISIONS

The concept of risk management is one which we believe may be useful in deciding what security practices are cost effective. This concept has been used by industry and Federal agencies--particularly the insurance industry--to make decisions regarding the costs of protecting against possible losses. The approach also has been advocated by NBS in its publication entitled "Guidelines for Automatic Data Processing Physical Security and Risk Management."

We are presenting a description of the approach here so it can be considered by agencies who undertake improvement in the physical security of their computer systems.

RISK MANAGEMENT

Risk management is an element of managerial science that is concerned with identification, measurement and control of uncertain events. This concept is not new, and portions have been used by organizations in quantifying needs when establishing business strategies. For example, one company used systematic risk analysis techniques to determine the extent of insurance coverage necessary for protection against product liability. This provided the company with a savings opportunity by assuming a \$5 million aggregate loss deductible on a \$6 million product liability insurance policy. In national defense, quantitative methods are used for analyzing risks to assure that proper safeguards are acquired and strategically implemented.

Portions of the risk management concept have also contributed to the insurance industry by providing greater flexibility in the type of insurance services offered for sale and wider ranges of insurance coverage at less cost to the industry. Risk management can also be used to determine an optimum level of security for data processing operations.

We contacted organizations referred to us as users of risk management techniques to determine security requirements. Some of these organizations considered factors used in risk evaluations but in most instances did not use a comprehensive risk management approach. Many leading

authorities in automatic data processing security are using various methods for analyzing risks, and they consider the following four phases essential for a formalized risk management approach:

- Risk analysis, management decision, risk control, and process continuity.

Risk analysis

Risk is the uncertainty of occurrence and outcome of specific events. Financially there are two basic types of risks.

- Speculative risks; an organization's investment of some or all of its assets with a degree of uncertainty as to whether the outcome will result in a gain, loss, or no change.

- Pure risks; unilateral events which could result in a loss of some or all of an organization's assets. Such losses are generally caused by physical destruction, misplacement, theft, fraud or adverse legal action. Uncertainty relates to whether or not a loss will occur; there is no opportunity in these instances for a financial gain. Threats against security in Federal data processing operations are considered as pure risks.

The initial planning for analyzing risks is to determine the extent necessary to carry out the analysis. Consideration should be given to the

- estimated costs and availability of funds to perform an analysis,
- value of the physical installation,
- worth of data to the organization and to others,
- existing safeguards, and
- impact of data processing on the organization's mission or goals.

Such considerations could dispose of the need for further detailed analyses. To illustrate, small computers used as calculators generally would not require extensive analyses because of their low cost and limited use for data storage.

Larger centralized time-sharing computer systems, however, would generally require risk analyses.

When a detailed analysis is warranted, all data processing assets such as computer equipment, software, and data, that are used to support a program or organizational goals must be identified and assigned a monetary value considering both the worth of the asset within and outside the organization.

An important phase in risk analysis is to identify all possible threats against assets. A risk audit is one technique used for this identification. A number of existing security checklists can serve as workable audit plans. Such audit plans should include interviews with key personnel, onsite inspections, as well as reviews of pertinent documents, records, and financial data to gain knowledge of operations and procedures and to identify the maximum number of threats involved.

Once known security threats have been defined, it is then necessary to postulate unknown threats and to measure the probability of occurrence for each threat. Some important parameters affecting such measurements and evaluations are

- cost and historical data on occurrence of various security threats,
- effectiveness of existing controls and procedures at an installation against each specific threat, and
- operating requirements both for the data processing activities as well as the organization.

Each type of security threat is unique and must be considered separately, as it can have a different impact on organizations. The levels of damage that can occur from each impact are referred to as loss severities. It is necessary to determine significant ranges of these severities for each threat. Once threats have been identified, it is then possible to determine the degree of loss and the impact of each loss on the installation's operating requirements as well as on the value of the facilities and data involved.

Management decision

The data gathered during the risk analysis phase can be summarized and presented to top management for consideration. This summary should relate threat assessments to

asset analyses and existing controls and show a relationship of each threat to the organizational mission and goals.

From this summary, management officials could then determine those risks that could be tolerated by the organization and those which require some control. Instances may occur when risk analyses indicate a reduction in security levels that are being maintained against certain threats, thus providing for reduced security costs. Other instances may show where the potential impact from risks combined with existing security techniques, if any, are acceptable to management. The only action necessary beyond this point would be to insure the effectiveness of techniques being employed.

Risk control

Once management determines that threats are unacceptable, the next phase is to control or avoid such risks by implementing an optimum degree of security relative to cost and operating requirements.

Risk handling techniques can be categorized as follows:

- Risk avoidance; a determination that the effects from threats and the probability occurrence is such that computerization is not warranted. Care must be taken with this decision to insure an ability to satisfy organizational needs with efficient and effective alternative solutions.
- Risk transfer; an organization's desires to shift some or all of its financial responsibility for risks to another party through contractual agreements.
- Risk assumption; a determination that it is more economical or operationally impractical to avoid the risk or transfer some portion of it to another party.

Federal Government policy is to absorb all financial losses incurred. Thus, specific methods must be identified to minimize the severity of a loss from each risk. Each method should be evaluated in terms of its effectiveness and cost and presented for management consideration.

Process continuity

Once security techniques have been implemented, they must be reevaluated periodically to determine their effectiveness in relation to the organization's mission and to the

program's computerized activity. During this analysis, management should be alert to the possibility that both existing or proposed security systems could be in excess of actual needs. This aspect could be assisted by the internal auditor. He would report his observations to the risk manager. When such instances are noted, consideration should be given to the potential for cost savings by reducing the degree of security being employed.

NEED FOR A RISK MANAGER

When computerized data serves the needs of more than one division or group, each program manager has a vested interest in the security of his data. If such a manager is permitted to establish separately his own security requirements, the resulting degree of security for data processing operations could become unmanageable.

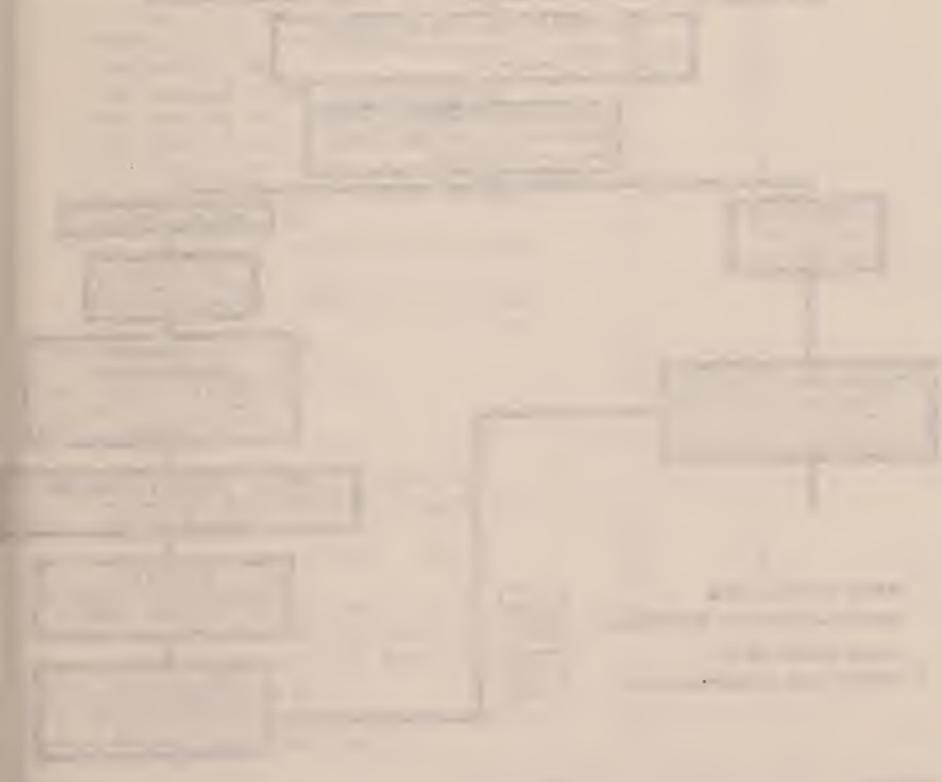
The initial step in establishing a risk management system is to create a position for a risk manager. The system is not likely to succeed without having one knowledgeable individual responsible for decisionmaking and supervision over all technical and analytical activities in the process. In small organizations, this position could be assumed as a collateral one by a top level management official. In larger and more complex entities, however, a separate position sufficiently high in an organization should be established for a risk manager to have authority for data processing security across organizational lines.

Some of the requisites for a top-level risk management position should be

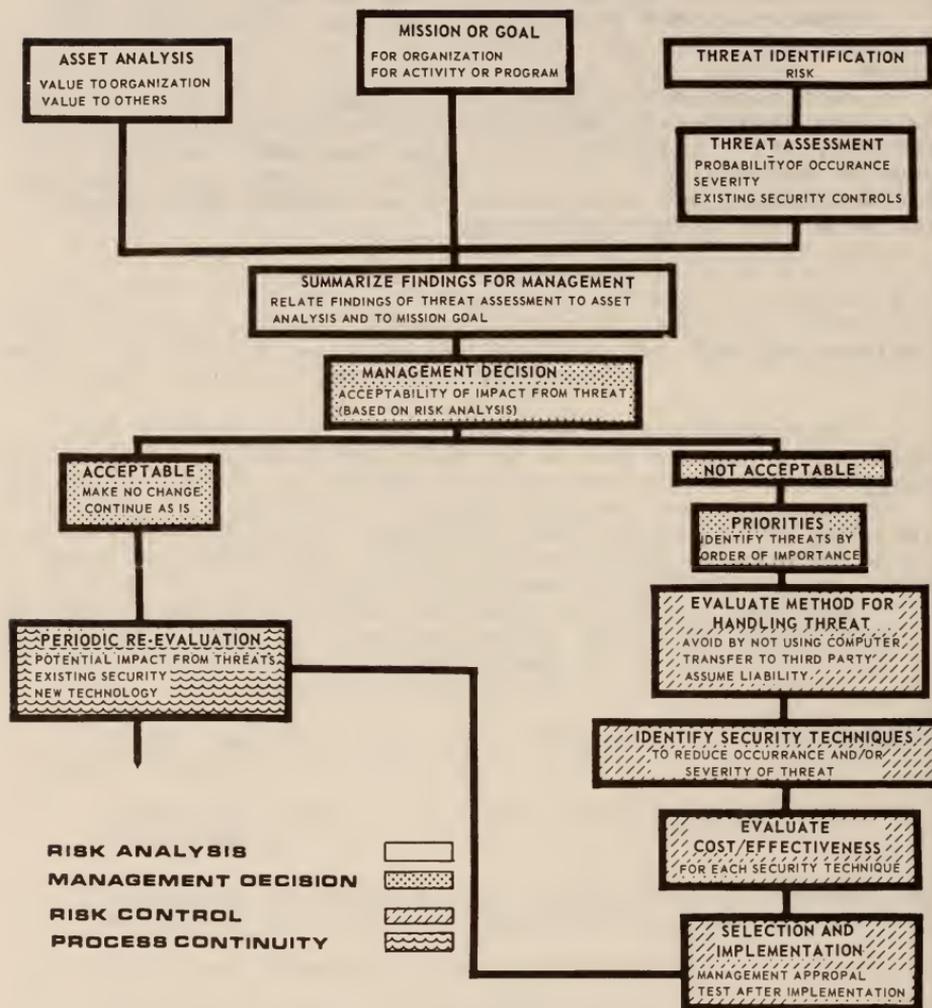
- knowledge of short- and long-range goals of the organization;
- awareness of users' security needs and priorities to establish and maintain appropriate levels of security;
- awareness of new technology for security;
- authority to make, or assist in making, policy decisions on security programs and procedures;
- authority, with management approval, to implement security measures deemed feasible from a risk analysis; and

--ability to follow through periodically on security policies and practices in action, checking actual performance and results.

Recognized authorities in risk management and automatic data processing security matters both in Government and industry agree that use of the risk management concept will provide methodologies and the systematic approach necessary for developing and maintaining proper levels of security for data processing operations.



CONCEPT OF RISK MANAGEMENT



SUMMARY OF SECURITY AREAS COVEREDAT 18 FEDERAL DATA PROCESSING INSTALLATIONS VISITED

	<u>Installations</u>		
	<u>Yes</u>	<u>No</u>	<u>N/A</u> <u>(note a)</u>
Access control:			
Is the location			
--target for vandals?	3	15	-
--advertised?	6	12	-
--screened from the street?	15	3	-
Are guards at entrances?	15	3	-
Are photo-badge systems used?	13	5	-
Are visitors controlled?	15	3	-
Do employees challenge unfamiliar visitors?	16	2	-
Are entrance security devices used?	11	7	-
Is access to computer limited during			-
--working hours?	17	1	-
--off-shift hours?	15	3	-
Fire exposure:			
Are fire resistant/noncombustible materials used for			
--buildings?	17	1	-
--partitions, walls, doors?	16	2	-
--furnishings?	15	3	-
Are smoke detectors installed?	11	7	-
Do the smoke detectors turn off air-conditioning facilities automatically?	6	5	7
Is the smoke detector system tested periodically?	7	4	7

a/Does not apply to installation and/or installation management that was reluctant to discuss these aspects of data processing security.

APPENDIX II

APPENDIX II

	Installations		
	<u>Yes</u>	<u>No</u>	<u>N/A</u> (note a)
Fire exposure:			
Do fire extinguishers use			
--automatic carbon dioxide?	2	16	-
--halogenated agent?		18	-
--water?	7	11	-
Are personnel trained for firefighting?	10	8	-
Is smoking restricted in computer area?	13	5	-
Are fire drills conducted regularly?	11	7	-
Are emergency power switches located at exits?	16	2	-
Do emergency power switches include air-conditioning system?	11	7	-
Flood control:			
Are computers located below water grade?	2	16	-
Do overhead steam or water pipes exist?	14	4	-
Does adequate drainage exist			
--under raised floors?	4	12	2
--on floors above?	1	14	3
--for adjacent areas?	4	12	2
Housekeeping:			
Are flammable materials properly stored?	18	-	-
Is area under raised flooring cleaned regularly?	4	12	2
Are paper and supplies stored outside computer room?	15	3	-
Are tapes and disks stored outside computer room?	8	9	1
Electric power:			
Is electrical power supply considered reliable?	18	-	-
Are voltmeters used to monitor supply?	8	10	-

APPENDIX II

APPENDIX II

	<u>Installations</u>		
	<u>Yes</u>	<u>No</u>	<u>N/A</u> <u>(note a)</u>
Air conditioning:			
Is air-conditioning dedicated to computer area?	16	2	-
Are backup air-conditioning facilities available?	5	13	-
Personnel considerations:			
Are employee background checks performed?	16	2	-
Are background checks updated periodically?	11	4	3
Is continuing education provided for security matters?	10	8	-
Is one person responsible for managing security?	13	5	-
Has security policy been developed?	15	3	-
Is in-house service personnel traffic			
--controlled in vital areas?	13	5	-
--supervised?	10	8	-
Is a list prepared for authorized vendor service personnel?	14	3	1
Is positive identification required for vendor service personnel?	15	2	1
Are vendor service personnel supervised while on premises?	10	7	1
Are vendor employee background checks verified?	5	8	5
Hardware considerations:			
Are hardware operations compared to scheduled activities?	14	1	3
Are meter hours correlated with reported utilization hours?	10	7	1
Are all periods of reported downtime verified?	17	-	1
Is all incoming work checked against an authorized users list?	13	3	2
Is output spot checked for possible misuse?	15	2	1

	Installations		
	<u>Yes</u>	<u>No</u>	<u>N/A</u> (note a)
Hardware considerations:			
Are output distribution lists updated periodically?	9	-	9
Are tapes cleaned at regular intervals?	10	6	2
Are tape utilization records maintained?	10	7	1
Is magnetic detection equipment used?	-	17	1
Software considerations:			
Is vital software and documentation secured?	14	3	1
Are backup files maintained at a secondary site?	12	5	1
Is access to essential software restricted on a need-to-know basis?	16	1	1
Is multilevel access control to files provided by			
--levels of security?	3	9	6
--breakdowns within files?	4	8	6
--restrictions for read-only, write-only, and update?	6	6	6
Are security software utilities and access codes validated periodically?	4	6	8
Is a monitor log maintained for those who access data banks or sensitive files?	2	8	8
Is a software security routine used to monitor unauthorized attempts to access files?	2	7	9
Are passwords utilized to identify users of terminals?	6	-	12
Are passwords changed frequently?	4	2	12
Are terminal users restricted to high-level languages?	2	4	12
Do operating systems have built-in protection to prevent the bypassing of other software security techniques?	2	8	8

	Installations		
	<u>Yes</u>	<u>No</u>	<u>N/A</u> <u>(note a)</u>
Software considerations:			
Are memory bounds in operating system software tested following maintenance and program loading?	5	6	7
Are restart and recovery procedures used in applications programs?	15	2	1
Do restart procedures operate on random as well as sequential files?	7	4	7
Are programing changes documented and controlled?	16	1	1
File considerations:			
Are duplicate program files stored offsite?	9	9	-
Are fire-resistant containers used for storage of program files?	13	5	-
Is a current inventory of program files maintained?	17	1	-
Have program files been tested on backup facilities within past 3 months?	7	10	1
Are computer programing changes controlled?	17	1	-
Are programing changes made on a duplicate rather than the original program file?	11	6	1
Are items taken from files recorded?	14	3	1
Are duplicate copies of documentation maintained?	13	5	-
Are copies of documentation stored offsite?	6	5	7
Is fire-resistant storage equipment used for documentation?	11	6	1
Are backup copies of documentation reviewed periodically to assure applicability?	12	4	2
Are all data files physically controlled by the computer center rather than the user?	10	8	-

	<u>Installations</u>		
	<u>Yes</u>	<u>No</u>	<u>N/A</u> <u>(note a)</u>
File considerations:			
Are data files classified by degree of sensitivity?	2	11	5
Are data files stored outside the computer room?	10	7	1
Is the storage area for data files fire protected?	9	6	3
Is access to storage area for data files specifically controlled?	7	9	2
Are fire-resistant containers used for storage of data files?	8	8	2
Resource sharing considerations:			
Are remote terminals used only by selected individuals?	4	1	13
Is access to remote terminals controlled by			
--locked doors?	1	4	13
--posted guards?	1	4	13
--other restraints?	3	2	13
Are passwords used to identify specific terminals and users?	6		12
Is password system considered tamperproof?	2	4	12
Are passwords changed frequently?	4	2	12
Is access to password file restricted?	6	-	12
Does system software restrict time sharing users to specific data files?	6	-	12
Is right to add, delete, or modify files limited by software controls?	6	-	12
Does time-sharing software record all activity against a data file?	3	3	12
Is there software protection for online operating systems and applications programs?	5	-	13

	<u>Installations</u>		
	<u>Yes</u>	<u>No</u>	<u>N/A</u> (note a)
Resource sharing considerations:			
Are security override procedures classified at the highest level and use of overrides monitored closely?	5	1	12
Is time-sharing security system monitored and reviewed?	3	2	13
Is debugging of security system closely monitored and controlled?	3	1	14
Contingency planning and backup:			
Does the installation have a formal written contingency plan?	9	8	1
Does the installation have a contingency training program?	5	8	5
Is a backup computer available?	7	11	-
Is the backup computer in the same room as the operating computer?	4	4	10
Can the backup facility handle the current workload?	4	6	8
If no designated backup, does center have access to another computer?	3	5	10
Is an implementation plan available for use of backup installation?	8	6	4

SUMMARY OF SELECTED SECURITY AREAS COVERED
AT OVERSEAS DATA PROCESSING INSTALLATIONS
VISITED

	<u>Installation</u>	
	<u>Yes</u>	<u>No</u>
Are buildings originally designed for computers?	1	9
Are supplies stored in a separate room?	7	3
Are fire extinguishers located in the computer room?	9	1
Are smoke or heat detectors installed in computer room?	6	4
Are fire alarm pull boxes located in computer room?	6	4
Are there master power shutdown controls for computer room?	<u>b/7</u>	3
Is emergency lighting installed in computer room?	8	2
Do buildings have water leakage problems?	5	5
Are separate air-conditioning facilities used for computers?	8	2
Are backup generators installed to insure reliability of electric power supply?	<u>c/7</u>	3
Have formal contingency plans been developed for computer backup capability?	4	6

b/One switch located in locked box, so not readily usable.

c/Backup generator at one location did not work at time of visit.

APPENDIX III

APPENDIX III



EXECUTIVE OFFICE OF THE PRESIDENT
 OFFICE OF MANAGEMENT AND BUDGET
 WASHINGTON, D.C. 20503

MAR 12 1976

Mr. D. L. Scantlebury
 Director, Division of Financial
 and General Management Studies
 General Accounting Office
 Washington, D.C. 20548

Dear Mr. Scantlebury:

We have reviewed GAO's draft report, "Federal Managers Need to Provide Better Protection for Automatic Data Processing Facilities," as requested in your letter of February 10, 1976; and believe that the report is useful in that it serves as a strong reminder to Federal managers on the importance of security measures for ADP facilities.

There is no question that Federal managers have a responsibility for protecting automatic data processing equipment and the associated software, as well as the data processed on this equipment from unauthorized use, acts of destruction, alteration or misuse. However, catastrophic losses to Federal data processing installations caused by flood, fire, explosions, etc. can never be completely eliminated. As stated in the report, "Perfect security is generally regarded as unattainable; therefore, the aim of a good physical security system should be to reduce the probability of loss to an acceptable low level of reasonable costs and to ensure adequate recovery in case of loss." We strongly support this concept of risk management.

It is our view that computer security should be viewed in the broader context of protecting agency installations, operations and records from a variety of potential threats and hazards and should not be treated separately. The head of each agency is already responsible for (1) assuring that the resources of his or her agency are properly protected (and necessary emergency back-up facilities and or services are available) to assure continued operation of critical agency activities; and (2) establishing whatever safeguards are appropriate to protect against threats to agency security. In the latter area, the concept of risk

management outlined in the Appendix I of your report has particular utility. Assistance and policy guidance is available to the agency from the Civil Service Commission (for personnel security) and from the General Services Administration (for building security and continuity of operations). Also, each major agency currently has a Security Officer whose responsibilities include personnel security as well as coordination with GSA on aspects of physical security within the building. We believe the agency head should be responsible for determining both the measures that are necessary, as well as how to organize to assure effective security; and question the appropriateness of directing that a separate official be named for ADP security.

Your report was generally supportive of the National Bureau of Standards guidelines on ADP physical security and risk management, but also indicated that improvements should be made in the guidelines.

We question whether it is necessary for OMB to issue any further policy directives at this time regarding application and use of the NBS guidelines. The responsibility and authority for developing, coordinating and issuing appropriate uniform ADP standards under the authority of P.L. 89-306 was delegated to the Secretary of Commerce by Executive Order 11717 dated May 9, 1973. The authority for developing any additional computer and data security standards that may be required to meet the requirements of the Privacy Act of 1974 (P.L. 93-579) were assigned to the Secretary of Commerce under OMB Circular No. A-108 dated July 1, 1975. While OMB recognizes and accepts its responsibility for policy formulation and oversight in these areas, we believe it would be more appropriate to direct specific recommendations on the improvement and strengthening of the existing guidelines and their use to the National Bureau of Standards of the Department of Commerce since they are the government's functional experts for this subject.

We share the view, implicit in the report, that there is a need for greater awareness of threats to physical security (particularly in ADP) and suggest that your final report address specific recommendations to those agencies you found to be lacking in adequate security

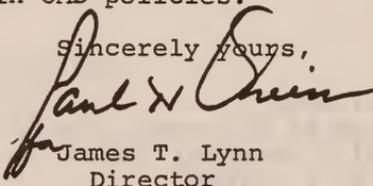
APPENDIX III

APPENDIX III

safeguards. We would also encourage wide dissemination of your report to each of the previously mentioned functional groups so that all concerned are adequately sensitized to this problem. We would be happy to assist in assuring that appropriate organizational elements within various agencies are made aware of the findings and conclusions of the final report.

We will continue to be supportive of the objective of this report and where appropriate will reflect ADP security requirements in OMB policies.

Sincerely yours,

A handwritten signature in dark ink, appearing to read "Paul H. Quinn". The signature is written in a cursive style with a large initial "P".

for James T. Lynn
Director

APPENDIX III

APPENDIX III



UNITED STATES DEPARTMENT OF COMMERCE
The Assistant Secretary for Administration
 Washington, D.C. 20230

17 MAR 1976

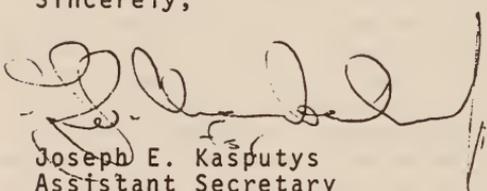
Mr. Victor L. Lowe
 Director, General Government Division
 U. S. General Accounting Office
 Washington, D. C. 20548

Dear Mr. Lowe:

This is in reply to your letter of February 11, 1976, requesting comments on the draft report entitled "Federal Managers Need to Provide Better Protection for Automatic Data Processing Facilities."

We have reviewed the enclosed comments of the Assistant Secretary for Science and Technology and believe they are responsive to the matters discussed in the report.

Sincerely,



Joseph E. Kasputys
 Assistant Secretary
 for Administration

Enclosure



APPENDIX III

APPENDIX III



UNITED STATES DEPARTMENT OF COMMERCE
The Assistant Secretary for Science and Technology
 Washington, D.C. 20230

Mr. Victor L. Lowe
 Director, General Government Division
 U.S. General Accounting Office
 Washington, D.C. 20548

Dear Mr. Lowe:

The GAO draft report, "Federal Managers Need to Provide Better Protection for Automatic Data Processing Facilities", sent to the Secretary for comment, contains numerous references to the National Bureau of Standards (NBS) publication "Guidelines for Automatic Data Processing Physical Security and Risk Management." In the large, the draft report is quite complimentary to the NBS guidelines. We are glad to have provided a vehicle which is of such importance to the Federal data processing community and would certainly undertake considering the recommendations for changes in the next edition of the guidelines.

One recommendation of the report is the appointment for each data processing facility of a management official responsible for automatic data processing (ADP) physical security and risk management. Page 38 of the report indicates that this management official should be outside of the ADP organization. This is not entirely clear in the recommendation. We infer that the attendant structure to support this person in all agency's substructures would also be necessary. This, coupled with the current requirement for privacy officers, represents fairly significant efforts. Consideration should be given to revising the recommendation so that physical security responsibility be assigned a person in the ADP organization with a physical security audit function established external to the ADP organization. This audit function would ensure the consistency and adequacy of the safeguards and procedures.

Thank you for this opportunity to comment on the draft report.

Sincerely,

Betsy Ancker-Johnson, Ph.D.





COMPTROLLER

ASSISTANT SECRETARY OF DEFENSE
WASHINGTON, D.C. 20301

15 MAR 1976

Mr. Donald L. Scantlebury
Director, Financial and General
Management Studies Division
U.S. General Accounting Office
Washington, D.C. 20548

Dear Mr. Scantlebury:

The Secretary of Defense has asked me to respond to your February 10, 1976 letter inviting comments on an enclosed GAO proposed report "Federal Managers Need to Provide Better Protection for Automatic Data Processing Facilities." This opportunity is appreciated and our comments follow hereafter.

The importance of the subject, the general substance of the report, and the thrust of the recommendations are wholeheartedly endorsed, subject to the following points:

1. The Digest on Page 1 refers to protection from ". . . unauthorized acts. . . ." It should also include "inadvertent acts."
2. The first recommendation pertaining to the appointment of an ADP physical security and risk management official, should explicitly call for him to be highly knowledgeable in ADP, as well as apart from the direct management of the ADP facility. This is required so as to provide the technical skill needed to recognize vulnerabilities while avoiding possible conflicts of interest.
3. The second recommendation should not require the NBS guidelines to be mandatory at this time. Their use as "Guidelines" rather than "Standards" was specifically selected after considerable deliberation by the Federal Information Processing Standards Coordination and Advisory Committee (FIPSCAC) in order to achieve an early dissemination of useful reference information which was not yet sufficiently developed to the point where they could undergo the more thorough coordination required for a mandatory standard. After further refinement, it is expected to become a standard but that point of maturation has not yet been reached. Further, DoD Directive 5200.28, "Security Requirements



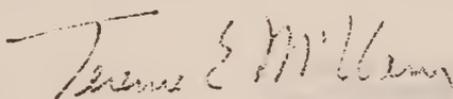
APPENDIX III

APPENDIX III

for ADP Systems," and DoD Manual 5200.28M, "ADP Security Manual," cover much of the same areas as the NBS guidelines. The substance of these documents, as well as documents from other agencies and industry, should be melded to provide a comprehensive set of concepts and guidelines for use of the government agencies in developing their respective policies.

I appreciate this opportunity to comment.

Sincerely,



Terence E. McClary
Assistant Secretary of Defense



DEPARTMENT OF HEALTH, EDUCATION, AND WELFARE
OFFICE OF THE SECRETARY
WASHINGTON, D.C. 20201

MAR 15 1976

Mr. Gregory J. Ahart
Director, Manpower and
Welfare Division
United States General
Accounting Office
Washington, D.C. 20548

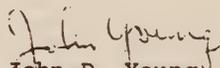
Dear Mr. Ahart:

The Secretary asked that I respond to your request for our comments on your draft report entitled, "Federal Managers Need to Provide Better Protection for Automated Data Processing Facilities."

We fully concur with the recommendations contained in the report (appointment of a management official responsible for ADP physical security and risk management, and establishment of policy dictating the use of NBS guidelines in those programs). In fact, this Department issued ADP Standards for ADP Systems Security in July 1975 which contain exactly these requirements.

We appreciate the opportunity to comment on this draft report before its publication.

Sincerely yours,


John D. Young

Assistant Secretary, Comptroller

APPENDIX III

APPENDIX III



OFFICE OF THE SECRETARY OF TRANSPORTATION
WASHINGTON, D.C. 20590

ASSISTANT SECRETARY
FOR ADMINISTRATION

March 12, 1976

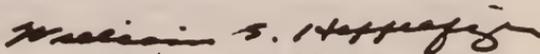
Mr. Donald Scantlebury
Director
Financial and General Management
Studies Division
U. S. General Accounting Office
Washington, D. C. 20548

Dear Mr. Scantlebury:

We have reviewed the draft report entitled "Federal Managers Need to Provide Better Protection for Automatic Data Processing Facilities." The Department of Transportation concurs with the draft report and the recommendations to designate a management official to be responsible for ADP physical security at each processing facility and to use the National Bureau of Standards' guidelines.

Editorially, we request that the reference to the "Federal Aviation Agency" on page 1 be changed to read "Federal Aviation Administration." Also, the reference to Public Law 93-597 on page 6 appears to mean the Privacy Act of 1974 which is Public Law 93-579.

Sincerely,


William S. Heffelfinger



**Federal Information
Processing Standards Publication 31**

1974 June



ANNOUNCING THE

**GUIDELINES FOR AUTOMATIC DATA PROCESSING
PHYSICAL SECURITY AND RISK MANAGEMENT**

Action Summary

The essential recommendations from this publication are summarized here to show the scope of these guidelines and to provide a quick overview of action items in establishing, implementing and maintaining a physical security program in an ADP facility.

I. Organize The ADP Physical Security Program

Assign responsibility for ADP Physical Security and establish a task force to prepare a plan for the ADP security program.

Perform a preliminary risk analysis to identify major problem areas and select interim security measures as needed to correct major problem areas.

II. Conduct A Risk Analysis

Estimate potential losses to the ADP facility and its users from (1) physical destruction or theft of physical assets; (2) loss or destruction of data and program files; (3) theft of information; (4) theft of indirect assets; and (5) delay or prevention of computer processing.

Estimate the probability of occurrence for potential threats and their effect on the ADP facility in terms of the five classes of loss potential.

Combine the estimates of loss potential and threat probability to develop an annual loss expectancy.

Select the array of remedial measures which effects the greatest reduction in the annual loss expectancy at the least total cost. Remedial measures will include: (1) changes in the environment to reduce exposure; (2) measures to reduce the effect of a threat; (3) improved control procedures; (4) early detection; and (5) contingency plans.

III. Determine Local Natural Disaster Probabilities

Evaluate the fire safety of the ADP facility (building location, construction, occupancy and housekeeping) and provide required fire detection and extinguishment, and possibly a trained fire fighting brigade.

Evaluate the exposure to flooding from internal and external sources. Where needed, provide flood protection for the building relocate ADP hardware, reroute plumbing lines and provide water damage/flood-control equipment (pumps, tarpaulins, etc.)

Evaluate resistance of the building to wind and water damage if exposed to hurricanes, tornadoes or other high winds.

FIPS PUB 31

IV. Initiate A Security Program

Prepare a plan and a schedule for implementing selected remedial measures. Prepare and maintain a policy and plans handbook to include: (1) an ADP physical security policy statement; (2) mandatory security procedures; (3) security guidelines for system design, programming, testing, and maintenance; (4) contingency plans; (5) security indoctrination materials; and (6) a security audit program.

V. Protect Supporting Utilities

Estimate the number and duration of electric power transients, undervoltage conditions and power interruptions and their annual loss expectancy. Install appropriate protective equipment such as: voltage regulating transformers, dual power feeders, uninterruptible power supplies, on-site power generators and ADP power isolation circuits.

Estimate annual loss expectancy from air conditioning failures considering required operation schedules, annual profiles of local temperature and humidity, and an estimated number and duration of air conditioning failures. Where necessary, increase reliability with redundant equipment, provide for emergency use of outside air and augment maintenance capability to decrease mean time to repair.

Estimate the annual loss expectancy from teleprocessing circuit failures. Where cost is justified, increase reliability with redundant communications circuits and augment repair facilities to decrease the duration of interruptions. Software should be designed to minimize the impact of errors caused by communications failures.

Determine if ADP operations could be interrupted by the failure of other supporting utilities such as water, natural gas, steam, elevators or mail conveyors. If necessary, take steps to increase reliability and decrease the mean time to repair.

VI. Optimize Computer Reliability

Perform a failure analysis to estimate the number and duration of significant hardware failures and their impact on ADP operations. Estimate the annual loss expectancy from delays in performing urgent ADP tasks. Where cost is justified, increase system reliability by adding peripherals, multiple configurations, etc. Review maintenance facilities. Record and analyze all hardware failures in order to identify failure trends promptly and optimize preventive maintenance.

VII. Provide Physical Protection

Identify critical ADP areas including the computer room, data control and conversion area, data file storage area, programmer's area, forms storage area, maintenance area, and mechanical equipment room, and then provide adequate physical protection and access control.

Protect against theft, vandalism, sabotage, espionage, civil disorder and other forced intrusions with improved lighting and intrusion detection systems, with physical barriers at doors, windows, and other openings, and with guards as required.

Control access to critical areas and ADP facilities with conventional or electronic door locks; supervision by guards or receptionists over movement of people and materials; administrative procedures (sign-in logs, identification cards or badges, property passes and shipping/receiving forms); and other regulations.

VIII. Add Internal Procedural Security

Determine potential targets for fraud, theft or misuse of resources by analyzing the work flow and the nature of ADP tasks performed. Incorporate procedures which will minimize exposure to loss. Such procedures may include (1) requiring cooperation between two individuals to perform critical tasks; (2) performing additional checks and bounds comparisons; (3) formalizing standards for high risk operations; and (4) independent quality control checks.

Designate critical positions in ADP management, system programming, program library control, input/output control, exception processing, applications programming, data base management, quality control, internal audit and hardware maintenance and require appropriate pre-employment screening.

Train and supervise all ADP personnel to assure understanding of, and compliance with, internal controls.

Implement control and record keeping procedures for job initiation, scheduling and distribution of output to prevent unauthorized processing.

Control access to physical data files to assure that data integrity is maintained, storage media are protected, custody of data files is traceable and their unauthorized use is prevented. Manual and automatic audit trails should be utilized.

Establish policy and procedures for program and data file retention to satisfy requirements for (1) back-up operation; (2) compliance with applicable statutes and regulation; (3) audit and management review of operation; (4) statistical analysis of operations; and (5) resolution of data integrity problems.

Implement programming, testing and documentation standards which satisfy requirements for (1) audit capability; (2) automated acceptance testing; (3) control program maintenance; (4) quality controls on input data; and (5) non-dependence on an individual's knowledge of systems and programs.

IX. Plan For Contingencies

Compile a set of back-up plans which accommodate the expected range of emergency events requiring back-up operation. The objective of such contingency plans is to protect users of the ADP facility against unacceptable loss. Document performance specifications, operation instructions and technical requirements (system hardware and software, program and data files, and preprinted forms) for each emergency operation.

Select and periodically use an emergency back-up off-site ADP facility. Participate in establishing their security program.

Provide protection for the source documents, input and output data and programs while using the off-site facility and in transit.

Establish procedures to assure that (1) current copies of needed back-up materials are retained at a secure off-site location; (2) adequate time is available from compatible off-site ADP facilities; and (3) back-up personnel will be available if needed.

Plan for reconstruction of the ADP facility following destruction including specifications of (1) floor space (quantity, live load rating, location, etc. by functional use); (2) partitions, electric power service, air conditioning, communications, security, fire safety, etc.; and (3) ADP hardware, office equipment and supplies.

Coordinate ADP emergency plans for fire, flood, civil disorders, etc. with the Facility Self-Protection Plan to ensure life safety, limit damage, minimize disruption to ADP operations, and expedite repair.

X. Develop Security Awareness

Determine the security training requirements for the ADP staff, senior management, building staff, etc.

Select and implement appropriate security awareness techniques such as (1) training lectures and seminars; (2) posters; (3) orientation booklets; (4) amendments to job descriptions making employees responsible for security; (5) publicity for local security incidents, as well as others occurring at similar installations; and (6) rewards for employees who prevent breeches in security.

Establish and publicize punitive measures.

IPS PUB 31

XI. Audit Physical Security

Establish an internal audit team with representatives from the agency's audit, building safety and security, ADP, and users' organizations.

Develop an audit plan and schedule which systematically validates all critical security and emergency measures.

State in the audit report which measures require improvement or replacement. Use a check sheet (problem description, responsibility for action, action required and follow-up) for each major deficiency to assure prompt resolution.

THE LIBRARY OF CONGRESS,
CONGRESSIONAL RESEARCH SERVICE,
Washington, D.C., June 11, 1976.

To Hon. Abraham Ribicoff, chairman, Senate Committee on Government Operations.

From: Louise Giovane Becker, analyst in information sciences.

Subj: Computer and information security in the Federal Government:
An overview.

In response to your request for information on computer crime and security measures we have prepared a brief overview and selected articles on these matters for inclusion in the projected committee print. In addition, a bibliography has been compiled of relevant books, articles, monographs, and documents.

The overview examines some of the issues and activities related to protecting computers and data from possible misuse or abuse. Although the stress here is on computer security and computer-related crimes it should be understood that privacy and related issues are not to be totally ignored. The interrelationship of privacy concerns and computer security must be considered in the light of recent Federal agencies' activities.

The articles selected for inclusion reflect the overall concern and interest in this subject. Most of the references fall into two categories—computer security and computer-related crime. The intent of the compilation is to provide an understanding of the key issues. Many of the items reflect the concern of both the technologists and administrators in coming to grips with problems associated with the security of computers and automated information systems.

The cited references in the bibliography are divided into four major categories—computer security, criminal use of computer technology, bibliographies, and general/miscellaneous. The references selected should provide additional information and an understanding of the scope and nature of the related problems.

In recent years the necessity in both the private and public sectors to develop cohesive plans in the management of computers has become increasingly evident. The increase in computer crime and the possibility of intentional or accidental abuse that would compromise the computer operations have required additional safeguards. More effective management of computer and information resources will be the key to future developments.

I. INTRODUCTION

Computers and automated information systems are vulnerable to all of the security problems of manual information and recordkeeping operations as well as to a wide range of abuses and misuses unique to their special characteristics and conditions. Protecting information

systems and their hardware requires an overall management concern and plan that includes the usual lock-and-key elements in addition to some special precautions.

Safeguards and security measures must be instituted that will protect the data processing facility, equipment (hardware), programs (software), data, and the integrity of the information. In other words, measures must include the protection of the entire operation. The level of protection must be in keeping with the data and operation to be protected and be consistently administered. The risk assessment must take into account the data and the scope and nature of the operation to be protected.

The focus of this memo will be primarily on overall Federal Government actions that reflect its interest in computer security and the prevention of computer crime. The activities of the intelligence community, while valuable to an understanding of computer security and risk assessment operations, will not be detailed in this discussion.

The extensive nature of the investment in and development of computer communication systems by the Federal Government is the major basis for instituting appropriate security measures. The Federal Government as the single largest user of computers, has well over 8,000 machines that provide a wide range of services and products essential to the welfare of the Nation. The handling, processing, and storage of data is key to many Federal programs and operations. Since computers and related technologies play a significant roll in the activities of a modern society it is essential that their utilization be properly controlled and managed. The misuse of these facilities, equipment, and data may have a serious impact on economic, political, and social activities of our citizens.

Some of the concepts and problems touched on here are presented in more detail a monograph by Peter S. Browne entitled "Computer Security—A Survey" which highlights some key technical problems and features an annotated bibliography.

Although some of the present activities regarding computer security stem from a concern for the privacy and protection of individual records, there has been consideration of the underlying issue—the management of information technology and resources. This focus is an essential and central issue in providing appropriate safeguards for computers and data handling operations. The cost of data processing operations and the importance to overall function of government agencies have placed special stress on the protection of information. Computer security has therefore become an essential and recognized aspect of managing information in the Federal Government.

DEFINITIONS FOR UNDERSTANDING

Computer security generally implies controlled access to both data and equipment. A few definitions are offered here to assist in providing an essential framework to understanding the issues and problems.

Security.—Is the protection of hardware, software, and data through the imposition of appropriate safeguards. Security comprises

data security, the protection of data against accidental or intentional destruction, disclosure or modification using both physical security measures and controlled accessibility, the set of technological measures of hardware and software available in a computer system for the protection of data.¹

Data.—A general term used to denote any or all facts, numbers, that refer to or describe an object or ideas, condition, situation, or other factors. It connotes basic elements of information which can be processed or produced by computer.

On-line.—Direct access to a computer or data bank so that information is available instantly through a remote terminal device or computer console.

Time-sharing.—The utilization of computer or data banks by many individuals from remote terminal devices at the same time.

Physical Security.—The detail protection of computers and facilities against penetration, destruction, and disruption.

Data and Systems Security.—Examines the development of computer programs (software) and systems design to insure that the systems is protected.

Computer Crimes.—Usually includes theft, fraud, and embezzlement with the use of computers and related technology.

Definitions of additional terms are included in the attached glossary prepared by the National Bureau of Standards as part of the Federal Information Processing Standards program.

II. BACKGROUND

Recent innovations and advances in technology have contributed to some of the problems of computer and information security. Computers permit efficient and economic storage, processing, and accessing of vast amounts of data. The development of large data bases with on-line (direct) access, has highlighted the need for better controls and safeguards. The increased use of remote terminals, video-screens, time-sharing, and browsing capabilities has stimulated the need to consider a re-assessment of access controls. In addition, the large dollar investment in both equipment and information has also encouraged the development of additional safeguards.

In less than three decades the computer has moved from the confines of the scientific laboratory to providing a wide range of services and products. It is generally recognized that computers are capable of handling diverse information problems—from complex space calculations to the design and ordering of parts; from manipulating simulation models to provide decisionmakers with alternatives to complex problems to assisting in issuing payments and invoices. The need to process vast amounts of data and the development of new computer applications have made Federal Government computer users increasingly dependent on this technology.

¹ Improving computer utilization. Computer technology at NBS. Dimensions, v. 57, Dec. 1973. p. 284.

As noted, most Federal Government programs and operations are highly dependent on the continued use of reliable computer and information systems. In recent years there has been a marked effort to develop appropriate safeguard guidelines which would optimize security in these systems. Computer security continues to be of concern to all elements of the Federal Government. In addition, the problem of protecting computerized information from criminal abuse has developed as an essential factor in the management of information handling systems.

Much of the initial interest and support for secure computers and systems has emanated from the military and intelligence communities. The sensitive nature of defense and national security information has fostered the development of secure systems in which planning and design carefully limit access. Sophisticated cryptologic (encoding devices), special hardware features, and unique software are employed to protect data and systems from unauthorized users. Many of the features of these security measures utilized by the defense and intelligence organizations have implications for the civilian sector as well.

A. GENERAL ACCOUNTING OFFICE REPORTS

Three reports issued by the Comptroller General's office, and included in this committee print, provide a review of some of the issues and problems related to computer security and crime. These reports focus on three significant problems in Federal systems—computer crimes, automated decisionmaking,² and the management of data processing facilities.

1. Computer Crimes in Federal Programs

The GAO report, "Computer-related Crimes in Federal Programs", highlights the potential vulnerability of Federal programs with regard to the use of "computer technology for fraudulent purposes". There is some difficulty in examining these problems due to the lack of adequate information. Federal agencies investigatory organizations often do not classify the crimes as such and therefore it is difficult to examine this problem. The report indicates that computer-related crimes coupled with an inappropriate use of computers have resulted in the need for Federal systems' managers to place more stringent controls on computer operations. The GAO recommends that specific measures be instituted to prevent criminal activities in computer systems. The report suggests that agencies undertake steps to prevent and discourage administrative and operational practices which might encourage computer crime activities.

A few articles have been included in the attached compilation that discuss the ways in which a computer served system can be penetrated and its data misused. Brandt Allen's article "Embezzler's Guide to the Computer" has been included in the compilation of articles because of its excellent survey of the vulnerabilities of computer systems

² Automated decisionmaking describes specific applications that induce a set of actions without manual supervision or intervention.

2. *Computerized "Automated Decisionmaking"*

Many Federal agencies have installed computer applications that include inventory ordering and invoice/payment systems. The GAO report, "Improvements Needed in Managing Automated Decisionmaking by Computers Throughout the Federal Government," examines some of the problems associated with automated decisionmaking and other associated problems of action directed computer programs. The GAO in reviewing some of these applications has called attention to the fact that poorly written programs and software often contribute to the difficulties. In addition, the study highlights the fact that unreviewed computer generated actions may cause the loss of billions of dollars in Federal Government assets.

3. *Managing and Safeguarding Federal Facilities*

The GAO report entitled "Managers Need to Provide Better Protection for Federal Automatic Data Processing Facilities" discusses the security policies and practices that could ultimately deter and prevent losses in Federal Government data processing operations. The study recommends that the Office of Management and Budget (OMB) support administrative changes and provide additional guidelines in the area of physical security and risk assessment management.

B. FEDERAL AGENCIES' RESPONSIBILITIES

Due to recent disclosures regarding government surveillance and related activities there is a growing awareness of and concern with government recordkeeping responsibilities. In brief, government accountability regarding the management of information has been demanded. Although the Privacy Act of 1974 concentrates only on systems that contain personally identifiable data it has stimulated thought regarding the need to better regulate and administer all information systems.

Federal Government ADP (automatic data processing) management has been a shared responsibility among the Office of Management and Budget (OMB), General Services Administration (GSA), National Bureau of Standards (NBS), and the Office of Telecommunication Policy (OTP). In addition, individual departments' and agencies' data processing elements have contributed to developing management guidelines.

C. LEGISLATIVE REQUIREMENTS

Over the years there has been continued concern in Congress with the management of information and recordkeeping function in the Federal Government. Over the years the management of information and computers has been continuously monitored by individual Members of Congress and various congressional committees. In addition, legislation has been proposed and enacted to promote good management practices. Two laws have contributed directly to improving computer security measures in the Federal Government; Public Law 93-306 the "Brooks Bill" and P.L. 93-579, the Privacy Act of 1974.

1. P.L. 89-306 the "Brooks Bill"

The improvement of ADP management has been encouraged both through legislation and administrative actions within the Federal Government. The "Brooks bill" enacted October 30, 1965, provided "for the economic and effective purchase, lease, maintenance, operation, and utilization of automatic data processing equipment by Federal departments and agencies".

The law provides that OMB exercise fiscal control and provide policy guidance, GSA is to be responsible for ADP equipment procurement and maintenance functions, the National Bureau of Standards is authorized to provide technological advisory services and establish ADP standards.

2. P.L. 93-579, *Privacy Act of 1974*

In the 93rd Congress, the Privacy Act of 1974 was passed to "safeguard individual privacy from the misuse of Federal records." The law permits individuals access to records maintained by Federal agencies concerning themselves.

Under the Act the Office of Management and Budget was designated to "develop guidelines and regulations for the use of the agencies" and to provide continuing assistance in the implementation of the Act. As an initial step OMB drafted guidelines to provide agencies with an overall framework within which to delineate specific administrative procedures in keeping with the law. In addition, the General Service Administration and the National Bureau of Standards were tasked by OMB to provide specific guidelines.

Specific provisions of the Privacy Act that relate to computer security include:

- limiting disclosure of personal information to authorized persons and agencies,
- requiring accuracy, relevance, timeliness, and completeness of records, and
- stipulating the use of safeguards to insure the confidentiality and security of records.

a. *General Services Administration (GSA)*

The GSA was requested to develop records management procedures to assist agencies in implementing the Privacy Act. These guidelines supplemented the OMB guidelines and regulations. The computer security requirements are to be evaluated prior to the procurement of new equipment or systems.

b. *National Bureau of Standards (NBS)*

NBS has concentrated on three categories of technical safeguards—physical security procedures, information management practices, and computer security/network controls. The Bureau has been active in encouraging the development of computer standards to improve the security and protection of automated data processing systems. Conferences have been held on computer security and risk assessment cost and economic aspects related to security have been studied, and guidelines on computer security standards have been issued. Other aspects of standards development will be discussed below.

NBS is responsible for a series of documents that provide standards and guidance, some of which are cited in the attached list of selected references. The "Executive Guide to Computer Security", which is among the documents in the compilation, provides some direction to those responsible for the oversight and management of information systems.

III. COMPUTER SECURITY AND STANDARDS

The development of computer standards and related symbolic conventions has been encouraged by both private and public sector elements. Standards have permitted the full utilization of computer resources, more uniform and effective products, and have increased the range of communications. Government, as one of the largest users of computers, has worked with industry to provide guidelines and stimuli requisite to the development of standards' development. Recent legislation and the need to better manage information resources have stimulated the development of ADP standards.

The authorization for the development of a Federal ADP standards program came about with the passage of P.L. 89-306 (Brooks bill). The National Bureau of Standards has had a leadership role in assisting government and non-government users in the development, implementation, and maintenance of data standards through Federal Information Processing Standards (FIPS) task groups. These groups, composed of interdisciplinary teams from government, industry, and other concerned elements, have provided a set of voluntary national standards to improve computer and information systems performance.

A. FIPS 15 COMPUTER SECURITY

One of the task forces concentrating its efforts on providing standards for computer security is Federal Information Processing Task Force 15 (FIPS 15).

Although the activities of this group actually began before the passage of the privacy legislation, it has since focused on those security requirements outlined in the Office of Management and Budget "Privacy Act" (P.L. 93-579) "Implementation Guidelines" FIPS 15 has developed a taxonomy of computer security requirements, a glossary, and a security risk assessment paper.

Robert A. Courtney's paper "Security Risk Assessment in Electronic Data Processing Systems", prepared as a working document for FIPS 15, outlines some of the problems and issues in selecting appropriate data security measures. Detailed examination of the risk assessment process and the methodology are included.

Computer security improvement in the Federal Government is dependent in part on the development and implementation of standards and other activities. Certain initiatives have been taken by the NBS in examining selected approaches improving computer security. They have issued a number of documents of risk assessment and computer security. In addition, NBS has provided a forum for the discus-

sion of the new standards, cost-aspects of security and privacy, and has continued to provide assistance in some instances to other Federal agencies. (See Bibliography and compilation for other material.)

IV. SUMMARY

As part of the overall concern for more effective and efficient use of modern technology computer security remains an important consideration. The possibility that computers can be used to perpetrate thefts and other criminal activity has provided an additional stimulus for improving risk assessment methods. Computer security is a necessary element in protecting data, software, equipment, and facilities from misuse. It is recognized that risk assessment activities and good management practices *must be combined* to provide maximum protection of the facility and its information.

The compilation of materials and references included in the committee print are intended to provide an initial framework for understanding the scope and nature of this complex problem. Federal Government must be responsive so that maximum protection is obtained at a reasonable cost. Safeguards and guidelines must also reflect the intent of existing legislation and congressional concern.

In reviewing ADP management practices, some important issues emerge that require additional consideration by Congress and other responsible Federal government elements.

One of the problems to be confronted is the call for total evaluation of ADP management practices in the Federal Government. Interested observers have often pointed to the lack of coordination and communication among Federal departments and agencies in planning and administering computer and information systems. There are indications that a more integrated approach to managing information systems may help to ensure that both economic and social factors are considered in the development of new systems.

Further investigation, undertaken in light of recent disclosures discussed in the GAO reports, might be required. The recommendations outlined in the reports and suggestions from other investigations must be considered. Some key issues have been identified that require further consideration by all responsible elements in Federal Government:

Should ADP management in the Federal Government be better organized and strengthened to ensure better use of resources?

Is there need for an indepth assessment of security and related concerns in the Federal Government?

Should further research be instituted on developing better performance measurements?

The re-evaluation of ADP management practices must occur within the context of expanded national information needs and the rapid emergencies of important innovations in technology. In the next few years Congress will consider programs such as national health care that will make unusual demands of our information handling practices. Therefore it becomes essential to have secure and well protected systems. In addition, as new services are initiated and old ones expanded, there will be a need for better government information support. This support must place special requirements on computer secu

rity elements to ensure the integrity of the system and to prevent computer abuse by those with criminal intent.

COMPUTER SECURITY AND CRIMINAL ABUSES OF SYSTEMS

SELECTED REFERENCES—1976

This bibliography is divided into four parts—physical and data security, computer crime, bibliographies and glossaries, and related references.

I. PHYSICAL AND DATA SECURITY

- Baird, Lindsay L., Jr. How to identify computer vulnerability. *Magazine of bank administration* v. 50, Oct. 1974: 16–21.
- Ball, Leslie D. and Wood, Steven D. Computer security in concentrated information systems. *Arizona business*, v. 23, 1976; 23–29.
- Bates, William S. Security of computer-based information systems. *Datamation*, v. 17, May 1970: 61–65.
- Beardsley, Charles W. Is your computer insecure. *IEEE spectrum*, v. 9, Jan. 1972: 62–78.
- Branstad, Dennis K. Data protection through cryptography. *Dimensions*, [National Bureau of Standards] v. 59, Sept. 1975: 195–197, 214.
- Browne, Peter S. Computer security—a survey. In the proceedings of the National Computer Conference 1976. New York, June 7–9, 1976 [New York, Association for Computing Machinery, 1976]. p. 129–1—129–11.
- Chacon, Jose A. Computer security. Perspectives in defense management, autumn 1973: 65–67.
- Chastain, Dennis R. Security vs. performance. *Datamation*, v. 19, Nov. 1973: 110–111, 116.
- Chu, Albert L. C. Computer security: the corporate achilles heel. *Business automation*, v. 18, Feb. 1, 1971: 32–39.
- Courtney, Robert H., Jr. Security risk assessment in electronic data processing systems. Poughkeepsie, New York, IBM Corporation, 1975. 81 p. (Revised December 1975.) “This report prepared as a working document for study and use by the Federal Information Processing Standards Task Group 15.”
- Del Castillo, Fernin Caro. Control in time-sharing systems. *Computers and automation*, v. 22, Nov. 1973: 10–13.
- Feistel, Horst. Cryptography and computer privacy. *Scientific American*, v. 228, May 1973: 15–23.
- Greenlee, M. Blake. William Brown, and Robert Jacobson. AMR's guide to computer security. New York, AMR [Advanced Management Research] International, Inc., [2d Printing] [1972] 208 p.
- Guard that computer. *National business* v. 59, Apr. 1971: 84–86.
- Hamilton, Peter. *Computer Security*. Philadelphia, Auerbach Publ. [1973] 122 p. HF5548. 2. H4475.
- Hemphill, Charles F. and John M. Hemphill. Security procedures for computer systems. Homewood, Illinois, Dow Jones-Irwin, Inc. [1973] 251 p. HF5548. 2. H362.

- Hirschfield, Richard A. Security in on-line systems—a primer for management. *Computers and automation*, v. 20, Sept. 1971: 15-17, and 25.
- Hoffman, Lance J. Security and privacy in computer systems. Los Angeles, Calif., Melville Pub. Co. [1973] 422 p. HF5548. 2. H484.
- International Business Machines. Considerations of data security in a computer environment. [White Plains, New York, 1972] 36 p. IBM no. G 520-2169.
- . The considerations of physical security in a computer environment. [White Plains, New York, 1972] [37] p. IBM no. G 520-2700-0.
- . Data security and data processing, v. 1-6. [White Plains, New York, 1972].
- Volume 1—Introduction and overview. 20 p. IBM no. G320-1370.
- Volume 2—Study summary. 25 p. G320-1371.
- Volume 3—Part 1 State of Illinois: executive overview. 43 p. IBM no. G320-1372.
- Part 2 Study results: State of Illinois. 438 p. IBM no. G320-1373.
- Volume 5—Study results: Massachusetts Institute of Technology. 300 p. IBM no. G320-1374.
- Volume 6—Evaluations and study experiences: Resource Security System. 121 p. IBM no. G320-1376.
- . 42 suggestions for improving security in data processing [White Plains, New York, 1973] 20 p. IBM no. G520-2700-0.
- Katzan, Harry Jr. Computer data security. New York, Van Nostrand Reinhold, Co. [1973] 223 p. HF5548.2K335.
- Kraus, Leonard I. SAFE security audit and field evaluation for computer facilities and information systems. East Brunswick, New Jersey, Firebrand, Krauss & Co. [1972] 284 p. HF5548.2.K683.
- Levin, Eugene. The future shock of information networks. *Astronautics and aeronautics*, v. 11, Nov. 1973: 52-57.
- Martin, James. Security, accuracy, and privacy in computer systems. Englewood Cliffs, N.J., Prentice-Hall, Inc. [1973] 626 p. HF5548.2.M342.
- Palme, Jacob. Software security. *Datamation*, v. 20, Jan. 1974: 51-55.
- Renninger, Clark R. ed. Approaches to privacy and security in computer systems. [Washington] U.S. National Bureau of Standards. [Washington, U.S. Govt. Print. Off.] 1974. 71 p. U.S. National Bureau of Standards. Special publication 404. "Proceedings of a Conference held at the National Bureau of Standards Mar. 4-5, 1974."
- and Dennis K. Branstand. Government looks at privacy and security in computer systems. [Washington] U.S. National Bureau of Standards, [U.S. Govt. Print. Off.] 1974. 37 p. U.S. National Bureau of Standards. Technical note 809. "A summary of a conference held at the National Bureau of Standards, Nov. 19-20, 1974."
- Turn, Rein. Privacy transformations for data bank systems. Santa Monica, Calif., Rand Corp. [1970] 47 p. Rand Corp. report no. P-4955.

- and H.R. Petersen. Security of computerized information systems. Santa Monica, Calif., Rand Corp. [1972] 9 p. Rand Corp. report no. P-4871.
- and Norman Z. Shapiro. Privacy and security in databank systems: measures of effectiveness, costs, and protector-intruder interactions. Santa Monica, Calif., Rand Corp. [1972] 36 p. Rand Corp. report no. P-4871.
- and Willis H. Ware. Privacy and security in computer systems. *American scientist*, v. 63, Mar.-Apr. 1975: 196-203.
- U.S. National Bureau of Standards. Federal Information Processing Standards Publication. Computer security guidelines for implementing the Privacy Act of 1974. (FIPS Publication, May 30, 1975) Category ADP Operations, Subcategory: Computer Security.) [Washington, U.S. Govt. Print. Off., 1974] 19 p. "FIPS Pub. 41."
- Guidelines for automatic data processing physical security and risk management. (FIPS Publication, June 1974. Category: ADP Operations, Subcategory: Computer Security.) [Washington, U.S. Govt. Print. Off., 1974] 92 p. "FIPS Pub 31."
- Van Tassel, Dennis. Computer security management. Englewood Cliffs, N.J., Prentice-Hall, Inc. [1972] 220 p.
- A contingency plan for catastrophe. *Datamation*, v. 17, July 1, 1974: 30-33.
- Information security in a computer environment. *Computers and automation*, v. 18, July 1969: 24-5, 28.
- Weiss, Harold. Computer security—an overview. *Datamation*, v. 20, Jan. 1974: 42-47.
- Wessler, John, Edith Meyer, and W. David Gardner. Physical security . . . facts and fancies. *Datamation*, v. 17, July 1, 1971: 34-35, 37.
- Woolridge, Susan, Colin R. Corder, and Claude R. Johnson. Security standards for data processing. New York, Wiley [1973] 186 p. HF5548.W655 1973.

II. COMPUTER-RELATED CRIME

- Adelson, Alan. Embezzlement by computer. *Security world*, v. 5, Sept. 1968: 26-27, 40.
- Alexander, Tom. Waiting for the great computer rip-off. *Fortune*, v. 90, July 1974: 143-146, 148, 150.
- Allend, Brandt. Embezzler's guide to the computer. *Harvard business review*, v. 53, Jul.-Aug. 1975: 79-89.
- Barnett, Chris. Vulnerability to computer fraud eyed. *Journal of commerce*, no. 9, 1973: 1a, 6a.
- Brenner, Lynn. In wake of Equity scandal interest in computer security mushrooms. *Journal of commerce*, May 19, 1975. 1.
- Deweese, J. Taylor. The trojan horse caper—and assorted other computer crimes. *Saturday review*, v. 3. Nov. 15, 1975: 10, 58-60.
- Espionage in the computer business. *Business week*, Jul 28, 1975: 60-62.

- Godbout, William. Computer theft by computer. *Security world*, v. 8, May 1971: 22-24.
- Grimes, John A. Equipty funding: fraud by computer. *American federationist*, v. 80, Dec. 1973: 7-10.
- Grosswirth, Marvin. How credit card crooks pick your pocket. *Science digest*, v. 77, June 1975: 58-65.
- How secure are your computers? *Industry week*, v. 186, Sept. 22, 1975: 40, 42-43.
- Irwin, T. K. The new computer crooks: the intricate schemes that net millions. *Washington family weekly*, (Washington Star News) April 7, 1974:
- Leibholz, Stephen W. and Louis D. Wilson. User's guide to computer crime: its commission, detection and prevention. Radnor, Pa. Chilton Book Co. [1974] H.R. 5548. 2. L393.
- Malloy, Michael T. Computer & thief-compucriminal. *The national observer*, Sept. 29, 1973: 1, 19.
- McKnight, Gerald. Computer crime. New York, Walker, 1974 c1973. 221 p. HV6768.M3 1974.
- Parker, Donn B. and Susan Nycum. The new criminal. *Datamation*, v. 20, Jan. 1974: 56-57.
- Parker, Donn B., Susan Nycum and S. Steven Oura. Computer abuse. Final report prepared for the National Science Foundation RANN NSF/RA/S-73-017. Menlo Park, Stanford Research Institute [1973] 131 p.
- Porter, W. Thomas, Jr. Computer raped by telephone. *The New York times magazines*, Sept. 8, 1974: 33-34, 36, 40-41, 43.

III. BIBLIOGRAPHIES AND GLOSSARIES

- Anderson, J. P. and Ed Fagerlaund. Privacy and the computer: an annotated bibliography. *Computing reviews*, 1972: 551-559.
- Begardt, Jeffery G., et. al. An annotated and cross-referenced bibliography on computer security and access control in computer systems. Columbus, The Computer and Information Science Research Center, Ohio State University [1972] 125 p.
- Harrison, Annette. The problem of privacy in the computer age: An annotated bibliography. December 1967. Santa Monica, Calif., Rand Corporation. [1967] 125 p.
- The problem of privacy in the computer age: An annotated bibliography. Volume 1. December 1969. Santa Monica, Calif., Rand Corp. [12969] 148 p.
- Hunt, M. K. and Rein Turn. Privacy and security in data bank systems: An annotated bibliography, 1969-73. 166 p.
- Liu, Yung-Ying, comp. Privacy and security in computer systems. Washington, Reference Section, Science and Technology Division, Library of Congress, 1974. 7 p. (U.S. Library of Congress. Science and Technology division. LC science tracer bullet, TB 74-7).
- Rittersback, George H. Data processing security: a selected bibliography. [Washington] U.S. Department of Commerce, National Bureau of Standards [1973] 11 p. NBS Technical Note 780.

U.S. National Bureau of Standards. Federal Information Processing Standards Publication. Glossary for computer systems security. Feb. 15, 1976. Category: ADP Operations, Subcategory: Computer Security. [Washington, U.S. Govt. Print. Off., 1976] 19 p.

IV. GENERAL AND MISCELLANEOUS

Chastain, Dennis R. Security vs. Performance. *Datamation*, v. 19, Nov. 1973: 110-111, 116.

Kraning, Alan. Wanted: new ethics for new techniques. *Technology review*, v. 70, Mar. 1970: 40-45.

Mandell, Mel. Computer scare talk. *New York Times*, May 9, 1971: 3F.

Nycum, Susan Hubbell. Computer abuses raise new problems. *American Bar Association journal*, v. 61, Apr. 1975: 444-448.

Peck, P. L. Jr. Environmental factors and threats to be considered in a computer security task. June 12, 1970. Revision 1, Cambridge, Mass., MITRE Corporation, 1970. (no paging).

Privacy and security: twin challenges to computer technology. *Dimensions*. (National Bureau of Standards) Jul. 1974: 147-149.

Reed, Susan K. and Dennis K. Branstad. Controlled accessibility workshop report. A report of the NBS/ACM Workshop on Controlled Accessibility. December 10-13, 1972. Rancho Santa Fe, Calif. [Washington, U.S. Govt. Print. Off., 1974] 81 p. NBS Technical Note 827.

Reed, Irving S. The application of information theory to privacy in data banks. Santa Monica, Calif., Rand Corp. [1973] 60 p.

Weinstock, C. B. A survey of protection systems. Pittsburgh, Pa. Carnegie-Mellon University, Department of Computer Science. [1973] 24 p.

SPECIFICATIONS OF THE GLOSSARY FOR COMPUTER SYSTEMS SECURITY

FOREWORD

The Federal Information Processing Standards Publication Series of the National Bureau of Standards is the official publication relating to standards adopted and promulgated under the provisions of Public Law 89-306 (Brooks Bill) and under Part 6 of Title 15, Code of Federal Regulations. These legislative and executive mandates have given the Secretary of Commerce important responsibilities for improving the utilization and management of computers and automatic data processing systems in the Federal Government. To carry out the Secretary's responsibilities, the NBS, through its Institute for Computer Sciences and Technology, provides leadership, technical guidance, and coordination of government efforts in the development of technical guidelines and standards in these areas.

The subject areas of computer security and data confidentiality are of the greatest national interest. The importance of a common vocabulary within these subject areas was recognized by the National Bureau of Standards and was given the highest priority by the Fed-

eral Information Processing Standards Task Group on Computer Systems Security. NBS is pleased to make this Glossary for Computer Systems Security available for use by Federal agencies as suggested definitions or interpretations of terms which are relevant in this area.

RUTH M. DAVIS,
*Director, Institute for Computer Sciences
 and Technology.*

access

The ability and the means necessary to approach, to store or retrieve data, to communicate with, or to make use of any *resource* of an ADP system.

access category

One of the classes to which a user, a program or a process in an ADP system may be assigned on the basis of the *resources* or groups of resources that each user, program, or process is authorized to use.

access control

The process of limiting *access* to the *resources* of an ADP system only to authorized users, programs, processes, or other ADP systems (in computer networks). Synonymous with controlled access, controlled accessibility.

access control mechanisms

Hardware or software features, operating procedures, management procedures, and various combinations of these designed to detect and prevent unauthorized *access* and to permit authorized access to an ADP system.

access list

A catalogue of users, programs, or processes and the specifications of *access categories* to which each is assigned.

access period

A segment of time, generally expressed on a daily or weekly basis, during which *access* rights prevail.

access type

The nature of an *access* right to a particular device, program or file, for example, read, write, execute, append, modify, delete, create.

accountability

The quality or state which enables violations or attempted violations of *ADP system security* to be traced to individuals who may then be held responsible.

accreditation

The authorization and approval, granted to an ADP system or network to process sensitive data in an operational environment, and made on the basis of a *certification by designated technical* personnel of the extent to which design and implementation of the system meet pre-specified technical requirements for achieving adequate *data security*.

active wiretapping

The attaching of an unauthorized device, such as a computer terminal, to a communications circuit for the purpose of obtaining *access*

to data through the generation of false messages or control signals, or by altering the communications of legitimate users.

add-on security

The retrofitting of protection mechanisms, implemented by hardware or software, after the ADP system has become operational.

administrative security

The management constraints, operational procedures, *accountability* procedures, and supplemental controls established to provide an acceptable level of protection for sensitive data. Synonymous with procedural security.

ADP system security

All of the technical safeguards and managerial procedures established and applied to computer hardware, software, and data in order to ensure the protection of organizational assets and individual privacy.

analysis

See *cost-risk analysis*; *cryptanalysis*; *risk analysis*.

approved circuit

Synonym for *protected wireline distribution system*.

audit

(1) To conduct the independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, and to recommend any indicated changes in controls, policy or procedures.

(2) The independent review and examination of system activities and records as in (1).

(3) See *external security audit*; *internal security audit*; *security audit*.

audit trail

A chronological record of system activities which is sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to each event in the path of a transaction from its inception to output of final results.

authentication

(1) The act of identifying or verifying the eligibility of a station, originator, or individual to *access* specific categories of information.

(2) A measure designed to provide protection against fraudulent transmissions by establishing the validity of a transmission, message, station, or originator.

authenticator

(1) The means used to identify or verify the eligibility of a station, originator, or individual to *access* specific categories of information.

(2) A symbol, a sequence of symbols, or a series of bits that are arranged in a predetermined manner and are usually inserted at a predetermined point within a message or transmission for the purpose of an *authentication* of the message or transmission.

authorization

The granting to a user, a program, or a process the right of *access*.

automated security monitoring

The use of automated procedures to ensure that the security controls implemented within an ADP system are not circumvented.

backup procedures

The provisions made for the recovery of data files and program libraries, and for restart or replacement of ADP equipment after the occurrence of a system failure or of a disaster.

between-the-lines entry

Access, obtained through the use of *active wiretapping* by an unauthorized user, to a momentarily inactive terminal of a legitimate user assigned to a communications channel.

bounds checking

Testing of computer program results for *access* to storage outside of its authorized limits. Synonymous with memory bounds checking.

bounds register

A hardware register which holds an address specifying a storage boundary.

brevity lists

A *code system* that is used to reduce the length of time required to transmit information by the use of a few characters to represent long, stereotyped sentences.

browsing

Searching through storage to locate or acquire information, without necessarily knowing of the existence or the format of the information being sought.

call back

A procedure established for positively identifying a terminal dialing into a computer system by disconnecting the calling terminal and reestablishing the connection by the computer system's dialing the telephone number of the calling terminal.

certification

The technical evaluation, made as part of and in support of the *accreditation* process, that establishes the extent to which a particular computer system or network design and implementation meet a prescribed set of security requirements.

cipher system

A *cryptographic system* in which *cryptography* is applied to *plain text* elements of equal length.

ciphertext

Unintelligible text or signals produced through the use of *cipher systems*.

code system

(1) Any system of communication in which groups of symbols are used to represent *plain text* elements of varying length.

(2) In the broadest sense, a means of converting information into a form suitable for communications or *encryption*, for example, coded speech, Morse Code, teletypewriter codes.

(3) A *cryptographic system* in which cryptographic equivalents (usually called code groups) typically consisting of letters, digits, or both in meaningless combinations are substituted for *plain text* elements which may be words, phrases, or sentences.

(4) See also *brevity lists*.

communications security

The protection that insures the authenticity of *telecommunications* and that results from the application of measures taken to deny unauthorized persons information of value which might be derived from the acquisition of telecommunications.

compartmentalization

(1) The isolation of the operating system, user programs, and data files from one another in main storage in order to provide protection against unauthorized or concurrent *access* by other users or programs.

(2) The breaking down of sensitive data into small, isolated blocks for the purpose of reducing risk to the data.

compromise

An unauthorized disclosure or loss of *sensitive information*.

compromising emanations

Electromagnetic emanations that may convey data and that, if intercepted and analyzed, may *compromise sensitive information* being processed by any ADP system.

concealment system

A method of achieving *confidentiality* in which the existence of *sensitive information* is hidden by embedding it in irrelevant data.

confidentiality

A concept that applies to data that must be held in confidence and that describes the status and degree of protection that must be provided for such data about individuals as well as organizations.

control zone

The space, expressed in feet of radius, that surrounds equipment that is used to process *sensitive information* and that is under sufficient physical and technical control to preclude an unauthorized entry or *compromise*. Synonyms with security perimeter.

controlled access

Synonym for *access control*.

controlled accessibility

Synonym for *access control*.

controlled sharing

The condition which exists when *access control* is applied to all users and components of a *resource-sharing* ADP system.

controllable isolation

Controlled sharing in which the scope or domain of *authorization* can be reduced to an arbitrarily small set or sphere of activity.

cost-risk analysis

The assessment of the costs of potential risk of loss or *compromise* of data in an ADP system without data protection versus the cost of providing data protection.

cross-talk

An unwanted transfer of energy from one communications channel to another channel.

cryptanalysis

The steps and operations performed in converting *encrypted* messages into *plain text* without initial knowledge of the *key* employed in the *encryption algorithm*.

cryptographic system

The documents, devices, equipment, and associated techniques that are used as a unit to provide a single means of *encryption* (*enciphering* or *encoding*).

cryptography

The art or science which treats of the principles, means, and methods for rendering *plain text* unintelligible and for converting *encrypted* messages into intelligible form.

cryptology

The field that encompasses both *cryptography* and *cryptanalysis*.

crypto-operation

See *offline crypto-operation*; *online crypto-operation*.

data contamination

A deliberate or accidental process or act that results in a change in the integrity of the original data.

data-dependent protection

Protection of data at a level commensurate with the sensitivity level of the individual data elements, rather than with the sensitivity of the entire file which includes the data elements.

data integrity

The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or malicious alteration or destruction.

data security

The protection of data from accidental or malicious modification, destruction, or disclosure.

data protection engineering

The methodology and tools used for designing and implementing data protection mechanisms.

decipher

To convert, by use of the appropriate *key*, *enciphered* text into its equivalent *plain text*.

decrypt

To convert, by use of the appropriate *key*, *encrypted* (*encoded* or *enciphered*) text into its equivalent *plain text*.

dedicated mode

The operation of an ADP system such that the central computer facility, the connected peripheral devices, the communications facilities, and all remote terminals are used and controlled exclusively by specific users or groups of users for the processing of particular types and categories of information.

degauss

(1) To apply a variable, alternating current (AC) field for the purpose of demagnetizing magnetic recording media, usually tapes. The process involves increasing the AC field gradually from zero to some maximum value and back to zero, which leaves a very low residue of magnetic induction on the media.

(2) Loosely, to erase.

eavesdropping

The unauthorized interception of information-bearing emanations through the use of methods other than wiretapping.

electromagnetic emanations

Signals transmitted as radiation through the air and through conductors.

emanation security

The protection that results from all measures designed to deny unauthorized persons information of value that might be derived from intercept and analysis of *compromising emanations*.

emanations

See *compromising emanations*; *electromagnetic emanations*.

encipher

To convert *plain text* into unintelligible form by means of a *cipher system*.

encode

To convert *plain text* into unintelligible form by means of a *code system*.

encrypt

To convert *plain text* into unintelligible form by means of a *cryptographic system*.

encryption

See *end-to-end encryption*; *link encryption*.

encryption algorithm

A set of mathematically expressed rules for rendering information unintelligible by effecting a series of transformations through the use of variable elements controlled by the application of a *key* to the normal representation of the information. Synonymous with privacy transformation.

end-to-end encryption

(1) *Encryption* of information at the origin within a communications network and postponing decryption to the final destination point.

(2) See also *link encryption*.

entrapment

The deliberate planting of apparent flaws in a system for the purpose of detecting attempted penetrations or confusing an intruder about which flaws to exploit.

entry

See *between-the-lines entry*; *piggy back entry*.

executive state

One of two generally possible states in which an ADP system may operate, and in which only certain privileged instructions may be executed; such privileged instructions may not be executed when the system is operating in the other, the user state. Synonymous with supervisor state.

external security audit

A *security audit* conducted by an organization independent of the one being *audited*.

failure access

An unauthorized and usually inadvertent *access* to data resulting from a hardware or software failure in the ADP system.

failure control

The methodology used to detect and provide fail-safe or fail-soft recovery from hardware and software failures in an ADP system.

fail safe

The automatic termination and protection of programs or other processing operations when a hardware or software failure is detected in an ADP system.

fail soft

The selective termination of affected non-essential processing when a hardware or software failure is detected in an ADP system.

fault

Synonym for *loophole*.

fetch protection

A system-provided restriction to prevent a program from *accessing* data in another user's segment of storage.

file protection

The aggregate of all processes and procedures established in an ADP system and designed to inhibit unauthorized *access*, *contamination*, or elimination of a file.

flaw

- (1) Synonym for *loophole*.
- (2) See *pseudo-flaw*.

formulary

A technique for permitting the decision to grant or deny *access* to be determined dynamically at access time, rather than at the time of creation of the *access list*.

handshaking procedures

A dialog between a user and a computer, a computer and another computer, a program and another program for the purpose of identifying a user and authenticating his identity, through a sequence of questions and answers based on information either previously stored in the computer or supplied to the computer by the initiator of dialog. Synonymous with password dialog.

identification

The process that enables, generally by the use of unique machine-readable names, recognition of users or *resources* as identical to those previously described to an ADP system.

impersonation

An attempt to gain *access* to a system by posing as an authorized user. Synonymous with masquerading, mimicking.

incomplete parameter checking

A system fault which exists when all parameters have not been fully checked for correctness and consistency by the operating system, thus making the system vulnerable to penetration.

integrity

See *data integrity; system integrity*.

interactive computing

Use of a computer such that the user is in control and may enter data or make other demands on the system which responds by the immediate processing of user requests and returning appropriate replies to these requests.

interdiction

The act of impeding or denying the use of system *resources* to a user.

internal security audit

A *security audit* conducted by personnel responsible to the management of the organization being *audited*.

isolation

The containment of users and resources in an ADP system in such a way that users and processes are separate from one another as well as from the protection controls of the operating system.

key

In *cryptography*, a sequence of symbols that controls the operations of *encryption* and *decryption*.

key generation

The origination of a *key* or of a set of distinct keys.

keyword

Synonym for *password*.

linkage

The purposeful combination of data or information from one information system with that from another system in the hope of deriv-

ing additional information; in particular, the combination of computer files from two or more sources.

link encryption

(1) The application of *online crypto-operations* to a link of a communications system so that all information passing over the link is *encrypted* in its entirety.

(2) *End-to-end encryption* within each link in a communications network.

lock-and-key protection system

A protection system that involves matching a *key or password* with a specified *access* requirement.

logical completeness measure

A means for assessing the effectiveness and degree to which a set of security and *access control mechanisms* meets the requirements of a set of security specifications.

loophole

An error of omission or oversight in software or hardware which permits circumventing the *access control* process. Synonymous with fault, flaw.

masquerading

Synonym for *impersonation*.

memory bounds

The limits in the range of storage addresses for a protected region in memory.

memory bounds checking

Synonym for *bounds checking*.

mimicking

Synonym for *impersonation*.

monitoring

See *automated security monitoring; threat monitoring*.

multiple access rights terminal

A terminal that may be used by more than one class of users; for example, users with different *access* rights to data.

mutually suspicious

Pertaining to the state that exists between interactive processes (subsystems or programs) each of which contains sensitive data and is assumed to be designed so as to extract data from the other and to protect its own data.

nak attack

A *penetration* technique which capitalizes on a potential weakness in an operating system that does not handle asynchronous interrupts properly and, thus, leaves the system in an unprotected state during such interrupts.

offline crypto-operation

Encryption or *decryption* performed as a self-contained operation distinct from the transmission of the encrypted text, as by hand or by machines not electrically connected to a signal line.

online crypto-operation

The use of crypto-equipment that is directly connected to a signal line, making single continuous processes of *encryption* and transmission or reception and *decryption*.

overwriting

The obliteration of recorded data by recording different data on the same surface.

passive wiretapping

The monitoring and/or recording of data while the data is being transmitted over a communications link.

password

A protected word or a string of characters that identifies or *authenticates* a user, a specific *resource*, or an *access type*. Synonymous with keyword.

password dialog

Synonym for *handshaking procedure*.

penetration

A successful unauthorized *access* to an ADP system.

penetration profile

A delineation of the activities required to effect a *penetration*.

penetration signature

(1) The description of a situation or set of conditions in which a *penetration* could occur.

(2) The description of usual and unusual system events which in conjunction can indicate the occurrence of a *penetration* in progress.

penetration testing

The use of special programmer/analyst teams to attempt to *penetrate* a system for the purpose of identifying any security weaknesses.

personnel security

The procedures established to insure that all personnel who have *access* to any *sensitive information* have the required authorities as well as all appropriate clearances.

physical security

(1) The use of locks, guards, badges, and similar administrative measures to control *access* to the computer and related equipment.

(2) The measures required for the protection of the structures housing the computer, related equipment and their contents from damage by accident, fire, and environmental hazards.

piggy back entry

Unauthorized *access* that is gained to an ADP system via another user's legitimate connection.

plain text

Intelligible text or signals that have meaning and that can be read or acted upon without the application of any *decryption*.

principle of least privilege

The granting of the minimum *access authorization* necessary for the performance of required tasks.

print suppress

To eliminate the printing of characters in order to preserve their secrecy; for example, the characters of a *password* as it is keyed by a user at an input terminal.

privacy

(1) The right of an individual to self-determination as to the degree to which the individual is willing to share with others information about himself that may be *compromised* by unauthorized exchange of such information among other individuals or organizations.

(2) The right of individuals and organizations to control the collection, storage, and dissemination of their information or information about themselves.

privacy protection

The establishment of appropriate administrative, technical, and physical safeguards to ensure the *security* and *confidentiality* of *data* records and to protect both security and confidentiality against any anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom such information is maintained.

privacy transformation

Synonym for *encryption algorithm*.

privileged instructions

(1) A set of instructions generally executable only when the ADP system is operating in the *executive state*; for example, the handling of interrupts.

(2) Special computer instructions designed to control the protection features of an ADP system; for example, the storage protection features.

procedural security

Synonym for *administrative security*.

procedures

See *backup procedures*; *handshaking procedures*; *recovery procedures*; *system integrity procedures*.

protected wireline distribution system

A *telecommunications* system which has been approved by a legally designated authority and to which electromagnetic and physical safe-

guards have been applied to permit safe electrical transmission of unencrypted *sensitive information*. Synonymous with approved circuit.

protection

See *data-dependent protection*; *fetch protection*; *file protection*; *lock-and-key protection system*; *privacy protection*.

protection ring

One of a hierarchy of privileged modes of an ADP system that gives certain *access* rights to the users, programs, and processes authorized to operate in a given mode.

pseudo-flaw

An apparent *loophole* deliberately implanted in an operating system program as a trap for intruders.

purging

(1) The orderly review of storage and removal of inactive or obsolete data files.

(2) The removal of obsolete data by erasure, by *overwriting* of storage, or by resetting registers.

real-time reaction

A response to a *penetration* attempt which is detected and diagnosed in time to prevent the actual penetration.

recovery procedures

The actions necessary to restore a system's computational capability and data files after a system failure or *penetration*.

remanence

The residual magnetism that remains on magnetic storage media after *degaussing*.

residue

Data left in storage after processing operations, and before *degaussing* or rewriting has taken place.

resource

In an ADP system, any function, device, or data collection that may be allocated to users or programs.

resource sharing

In an ADP system, the concurrent use of a *resource* by more than one user, job or program.

risk analysis

An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of the occurrence of those events.

sanitizing

The *degaussing* or *overwriting* of *sensitive information* in magnetic or other storage media. Synonymous with scrubbing.

scavenging

Searching through *residue* for the purpose of unauthorized data acquisition.

scrubbing

Synonym for *sanitizing*.

secure configuration management

The use of procedures appropriate for controlling changes to a system's hardware and software structure for the purpose of insuring that such changes will not lead to a decreased *data security*.

secure operating system

An operating system that effectively controls hardware and software functions in order to provide the level of protection appropriate to the value of the data and *resources* managed by the operating system.

security

See *add-on security; administrative security; communications security; data security; emanation security; personnel security; physical security; procedural security teleprocessing security; traffic flow security*.

security audit

An examination of *data security* procedures and measures for the purpose of evaluating their adequacy and compliance with established policy.

security filter

A set of software routines and techniques employed in ADP systems to prevent automatic forwarding of specified data over unprotected links or to unauthorized persons.

security kernel

The central part of a computer system (software and hardware) that implements the fundamental security procedures for *controlling access* to system *resources*.

security perimeter

Synonym for *control zone*.

seepage

The accidental flow, to unauthorized individuals, of data or information *access* to which is presumed to be controlled by computer security safeguards.

sensitive information

Any information which requires a degree of protection and which should not be made generally available.

spoofing

The deliberate inducement of a user or a *resource* to take an incorrect action.

supervisor state

Synonym for *executive state*.

system

See *cipher system; code system; concealment system; cryptographic system; lock-and-key protection system; protected wireline distribution system; secure operating system*.

system integrity

The state that exists when there is complete assurance that under all conditions an ADP system is based on the logical correctness and reliability of the operating system, the logical completeness of the hardware and software that implement the protection mechanisms, and *data integrity*.

system integrity procedures

The procedure established for assuring that the hardware, software, and data in an ADP system maintain their state of original integrity and are not tampered with by program changes.

technological attack

An attack which can be perpetrated by circumventing or nullifying hardware and software *access control mechanisms*, rather than by subverting system personnel or other users.

telecommunications

Any transmission, emission, or reception of signs, signals, writing, images, sounds or other information by wire, radio, visual, or any electromagnetic systems.

teleprocessing

Pertaining to an information transmission system that combines *telecommunications*, ADP systems, and man-machine interface equipment for the purpose of interacting and functioning as an integrated whole.

teleprocessing security

The protection that results from all measures designed to prevent deliberate, inadvertent, or unauthorized disclosure, acquisition, manipulation, or modification of information in a *teleprocessing* system.

terminal identification

The means used to establish the unique identification of a terminal by an ADP system.

threat monitoring

The analysis, assessment, and review of *audit trails* and other data collected for the purpose of searching out system events which may constitute violations or precipitate incidents involving data *privacy* matters.

time-dependent password

A *password* which is valid only at a certain time of the day or during a specified interval of time.

traffic flow security

The protection that results from those features in some crypto-equipment that conceal the presence of valid messages on a communications circuit, usually by causing the circuit to appear busy at all times, or by *encrypting* the source and destination addresses of valid messages.

trap door

A breach created intentionally in an ADP system for the purpose of collecting, altering or destroying data.

trojan horse

A computer program that is apparently or actually useful and that contains a *trap door*.

validation

The performance of tests and evaluations in order to determine compliance with security specifications and requirements.

wiretapping

See *active wiretapping, passive wiretapping*.

work factor

An estimate of the effort or time that can be expected to be expended to overcome a protective measure by a would-be penetrator with specified expertise and *resources*.

SECURITY RISK ASSESSMENT
IN
ELECTRONIC DATA PROCESSING SYSTEMS

by
Robert H. Courtney, Jr.
Revised December 1975

This report was prepared as a working document for study and use by the Federal Information Processing Standards Task Group 15, Computer Systems Security, of the United States Department of Commerce National Bureau of Standards. It does not have the approval or endorsement of that group. Further, its publication by the IBM Corporation is in support of FIPS TG-15 activities and should not be interpreted as a specific endorsement by IBM of the material herein.

IBM CORPORATION
P.O. Box 390
POUGHKEEPSIE, NEW YORK 12602

CONTENTS

1.0	Introduction.	5
2.0	The Two Principal Factors	7
3.0	The Methodology	12
4.0	Helpful Hints	16
5.0	The Risk Analysis Team.	18
6.0	An Example.	20
7.0	Considerations In The Selection Of Security Measures. . .	32
8.0	Bibliography.	79

ABSTRACT

Concern for the safety of a data processing facility and the data within it should result in the selection of such security measures, including insurance, as are appropriate to bringing the risk within tolerable limits at the lowest costs. Security measures to do this should be selected on the basis of the benefit/cost relationships which they afford. This, in turn, requires a quantification of the potential benefits afforded by the security measure for comparison with its cost. Because the benefits afforded by the security measure is lessening or elimination of security problems, which is, risk reduction, we must be able to quantify the risk so as to measure the benefit afforded by its elimination or diminution. A workable procedure for doing this is described.

1.0 INTRODUCTION

Most management decisions involve the assumption of risk - the chance that things may not turn out the way we hope or want them to. Decisions made in spite of uncertainties and, indeed, in recognition of them are generally accepted as essential to dynamic, successful management. Most frequently, however, the key to success lies not in the willingness to accept uncertainty, or to assume risk, but in the ability to recognize and quantify the elements of that risk so as to deal with them in a fully objective way. Virtually every manager must come to grips with and manage risk in some form. For this reason, risk management has become recognized as a distinctly identifiable function of general organization or project management.

Concern for the safety of a data processing facility and the data within it should result in the selection of those security measures, including insurance, which are appropriate for bringing the risk within tolerable limits at the lowest costs. The measures to do this should be selected on the basis of the benefit/cost relationships which they afford. This, in turn, requires a quantification of the potential benefits afforded by the security measure for comparison to its cost. Because the benefit afforded by a security measure is the lessening or elimination of security problems, that is risk reduction, we must be able to quantify the risk in order to measure the benefit afforded by its elimination or diminution.

The steadily growing dependence of virtually every kind of organization on electronic data processing systems has introduced new concerns, which themselves have grown rapidly in the past few years. These concerns are attributable to a wide variety of factors, but there are two principal ones. First is the recognition of the recent rapid growth in the centralization of the data keeping and information extraction processes, with the attendant potential for the loss of the entire facility or major portions of it. Such loss might result in a severe set-back for the organization. The second major factor is recognition of the increasing dependence of the enterprise on employees with skills, talents, and disciplines, and sometimes motivations, quite different from those with which management has been familiar in the past. There is a feeling that these people might present new, unfamiliar problems and unfamiliar problems generally yield more discomfort than do familiar ones.

This paper was prepared in response to a clear need for a rational, systematic approach to a quantitative analysis of the security risks associated with electronic data processing systems. There has been broad agreement for some time that a risk analysis technique is needed, but no readily workable,

broadly applicable technique has been described in sufficient detail for it to be in general use. A methodology is offered here for assessing the risks specific to an organization, the particular system within that organization, and, to the extent necessary, the specific entities of which each system is comprised. More specifically, the purpose of this document is to describe one way of doing a risk analysis, that is, quantifying security problems, which has been found workable by several organizations.

Earlier versions of this paper provoked active discussion of the precise nature of those undesirable things which should be considered appropriate topics for risk assessment. Opinions ranged from a belief that consideration should be given only to catastrophic events, which would result in a complete loss of the data processing capability, to the opinion that only events ascribable to intentional misconduct need evaluation. At the opposite extreme, some held the position that consideration must be extended to all things which might result in undesired modification, destruction, or disclosure of data or suspension of data processing services. The latter is the correct approach. While this will increase the work required to complete the risk analysis, there is no basis for a priori exclusion from consideration of subsets of the total array of undesirable things which can happen to data and data processing capabilities. It is not until the impact of the event and its frequency of occurrence have both been examined, which is in fact a risk assessment, that there can be a reasoned justification for the exclusion from further consideration of any potential source of damage.

It has been argued that the inclusion into the relatively formal risk analysis procedure of such things as data entry errors, mistakes in handling tapes, and operator errors is an invasion of the normal province of the data processing manager. It can also be viewed as a tool to assist him in the identification of the need for and selection of appropriate safeguards.

The purpose of performing a risk assessment is to obtain a quantitative statement of the potential problems to which the data processing facility is exposed, so that appropriate, cost-effective security safeguards can be selected. It is assumed that, once armed with such information, no security measure will be selected which costs more than tolerating the problem. The risk assessment, should establish that threshold.

Section 2 is included to provide a discussion of the various security measures, other than physical and procedural, which might be considered in a program of assessing candidate security measures which will either reduce the cost of problems which have been evaluated in the risk assessment process or lower their probability of occurrence. The specific cost of any particular combination of measures is so much a function of the many variables associated with the specific facility that no definite statements of cost can be made here.

2.0 THE TWO PRINCIPAL FACTORS

Most people who have seriously considered or attempted to devise a risk analysis procedure, readily agree that useful technique must yield a quantitative statement of the effect, or impact, of specific security problems. However, there is less than uniform agreement that the unit of measure can or should be monetary. In addition to a measure of impact, a statement of the probability of the occurrence of a particular event is essential to a useful risk assessment. We contend that the two key elements in risk analysis are:

1. A statement of impact, that is, how badly a specific difficulty hurts.
2. A statement of the probability of encountering that difficulty in a specified period of time.

Both parameters are needed to describe risk in terms of cost per unit time, such as dollars per year.

The probability of an undesirable thing happening is usually more difficult to determine with confidence than is a measure of the impact of its happening. It has been suggested that we are so accustomed to making unconscious, gross, subjective judgments of probability in reaching decisions that it is difficult to accept a formalization of the process. Whatever the reasons for finding it difficult, statements of the potential economic impacts of events without regard to their relative probability, cannot lead to the identification of those security exposures that are worthy of corrective action and those which are not. There are, of course, many events which could have catastrophic consequences but which appear to have such low probability of happening as to not justify the expenditure of significant resources to lessen the potential damage. For example, at another time and in another social climate, we judged the probability of nuclear attack to be sufficiently high that we were persuaded to provide and stock fallout shelters. We have now, for the most part, abandoned those shelters, not because the damage which would be caused by such an attack is believed lower, but because we judge the probability of attack to be too low to justify the cost, in dollars and inconvenience, of maintaining these facilities. Our decision to abandon a security measure was based on a reassessment of the probability of occurrence - not on cost impact.

As another example, assume that a hypothetical major corporation has centralized most of its data processing facilities into a single location. Also assume that no plans have been made for data processing support elsewhere in the event of a catastrophic

loss of that facility. Suppose that the sum of all costs to the corporation of such a loss is, at first estimate, \$150 million, including not just the replacement costs of hardware, but also lost business opportunities, customer ill-will, interruption of proper cash management, and other key activities. As such, the availability of the \$150 million figure, while possibly interesting, does not lend itself to any real measure of the problem. It does not suggest how much might reasonably be spent in reducing the exposure. If we then determine, through further analysis, that we might reasonably expect such a loss with a frequency of .003/year, we do have a basis for a decision on corrective action. It is clear that we have an exposure in the order of \$450,000/year.

Continuing our example, we have three options in addressing the exposure; we can:

1. Tolerate it.
2. Lower the dollar impact by implementing those measures which cost less than a total of \$450K per year, if any.
3. Lower the probability of the loss occurring by implementing protective measures costing less than the exposure.

The point made here is that, unless we had quantified both the impact and the probability of occurrence, we would not be in a position to make an informed election of any of the three options.

Parenthetically, it should be noted that insurance is not a fourth option. Insurance provides a means of smoothing the impact of the loss when and if it happens. As such, it is a matter to be considered after the election of the other options. The availability of insurance does not necessarily lessen the desirability of minimizing risk by other measures. The downward adjustment of risk should lessen the amount of insurance required (in the case of reduced impact) or the rate (in the case of reduced probability or occurrence). In the unlikely event that such reductions do not change the cost of insurance, this should affect either the decision to insure or the decision to apply security measures.

It was stated earlier that there is something less than complete agreement that the impact of security problems is best measured in dollars. Those people who seem to have the most difficulty in assigning dollar values to security problems are, for the most part, either:

1. Considering the safety of data collections which, if disclosed or otherwise harmed, would have some identifiable and undesirable political or social ramifications, and are possibly affected by privacy legislation.

2. Have an involvement with defense or intelligence activities. The risks associated with activities in these two categories are generally much more difficult to assess quantitatively than are many other exposures. However, this does not lessen the desirability of such assessment.

The reluctance to use dollars as a means of sizing the negative social impact of security problems is understandable. It must be anticipated that many people will not look kindly on those that appear coldly to assess in dollars the hurt which might befall people as a consequence of some security problem which impacts those people personally. The appearance of an objective measurement in dollars, for example, of an individual's privacy concerns might be abhorrent to many people. This reluctance to use dollars as the measure has led to several parallel development efforts to define the severity of problems in these categories using relative sensitivities as, for example, on a scale of 1 to 5. Such rating schemes are valuable and their use should be encouraged. They are means of communicating an assessment of the potential for harm to people of the loss of security to files of specific types. For example, a rating of "1", indicating great sensitivity, for psychiatric data and "2" for files containing personal data which is a little less sensitive, such as tax files. Such ratings do not, however, provide an adequately meaningful parameter for guidance in the selection of economically feasible security measures. Such rating schemes can, and should coexist with risk analysis techniques which quantify the problem in dollars.

It is conceivable that a convention which uses relative sensitivities on a scale of 1 to 5 can be coupled with another which describes probability of occurrence to provide an expression which says that the probability of a 2-sized problem is 0.3/year. However, this does not provide much help in evaluating the need for or relative effectiveness of specific security measures.

A specific security measure is often difficult to justify in terms of its ability to contain only one problem, and the best security measures are usually those which contain or assist in containing more than one.

Any summation of risks contained by a specific measure or combination of measures requires that these risks be expressed in common units of measure. If some problems are describable only in economic terms and others in non-dimensional sensitivity ratings, the ability of specific measures to contain a variety of problems will be awkward to assess and security measures difficult to cost-justify.

Much of the problem of quantifying subjective concerns often seems to go away if, in performing the risk analysis, we

defer until last the decisions we do not know how to make. It then frequently becomes clear that other, more easily quantifiable concerns fully justify the required security enhancements.

As an example, it is usually difficult to arrive at a quantitative statement of the privacy impact of an exposure of the violations records associated with vehicle operators' license files. That such data are generally public record does not lessen belief that their consolidation in a machine-based system results in potential for their unfair exposure to too many people who should not or do not need to see them. The clear need to protect such data against unauthorized, accidental or intentional (illegal) modification will justify a level of security sufficiently high to displace concerns for disclosure as the dominant factor in selecting security measures.

It is not argued that serendipity will always prevail in such matters, but there is no reason to ignore any assistance that it might provide. The present limited experience in applying this risk analysis methodology to data collections where social concerns are of major importance leads to the strong belief that data security considerations other than protection against disclosure will often dictate security measures adequate for protection against disclosure and thus relieve the need for solid quantification of the social impact, real or imagined.

While those considering the problem of social impacts of losses of data security have trouble expressing in dollars the damage which might be done to people, the defense establishments and have a greater problem in addressing the other factor in the risk analysis expression, the probability of occurrence.

It is usually not easy to assess the dollar implication of losses of classified data or denial of processing capability. An even greater problem is encountered when trying to assess the probability of espionage and sabotage. Because the losses in such cases can be very great, it becomes difficult to accept as tolerable any probability of occurrence. This dilemma leads to such logical dead ends as the statement that "if it can happen, we must assume that it will happen with a probability of 1".

There is no really sound basis for the assignment of specific values to the probability of espionage or other illegal conduct relative to the security of military or intelligence data. This does not justify the assumption of meaningless extremes, because the result of this approach is an irrational or, at best, highly subjective response to the problem.

The use of electronic data processing capabilities in the handling of classified data has complicated security more by introducing problems which are not well understood than by increasing the actual severity of these problems. Most approaches used today, as in the past, to protect classified data, with a few notable exceptions, are wholly pragmatic and are based on simple "reasonable person" criteria. Their selection and application are heavily influenced by the level of interference which operations can tolerate. It is not suggested that this is wrong. It may be the only way when the probabilities are not knowable. The workability of this approach should be remembered when first considering security in data processing operations involving classified data.

It is important to avoid the inclination to overemphasize the significance of technical problems simply because their solutions are intellectually challenging. Frequently, the more intellectually stimulating problems are also those with low probabilities of occurrence. The probability of occurrence of these more exotic problems is lowered by the limited number of people in a position to pose each specific problem. Thus, we are more inclined to concern for the potential for damage by a systems programmer, of whom there are relatively few, but whose capabilities provide quite challenging problems, than we are to a critical evaluation of the effectiveness of a guard force in keeping strangers, of whom there are many, out of a facility and in restraining persons from carrying out what they should not remove from the premises, including media for data storage.

In many electronic data processing environments, the number of people in a position to do damage tends to be inversely proportional to the amount of damage which they might do. This is desirable and should be a goal of those concerned with the security of these facilities. Unfortunately, this comment does not apply to many other security-sensitive environments not involving electronic data processing.

The great majority of systems in both government and the private sector fortunately do not have their security needs dominated by unquantifiable events or probabilities or probabilities of occurrence due to undefined potential social impact or defense problems. Even in systems free of these problems, it may at times be difficult to arrive at precise assessments of event impact or probability. It is usually quite feasible to arrive at figures which, while inexact, are good enough for the purpose of evaluating exposures and for guidance in selecting appropriate security measures.

3.0 THE METHODOLOGY

The proposed risk analysis procedure proposed is almost completely described by the sample form shown as figure 1. The form is for use in evaluating the risk of damage to data from all causes, including its loss to physical threats, such as fire.

Data security problems are those which result from the accidental or intentional, but unauthorized, disclosure, modification, or destruction of data or the loss of the ability to process it. There are, then, six bad things which can happen to data and, in addition to those six, there can be the denial of processing capability. It is important that all six be kept in mind because security measures to be fully cost effective need to address the broadest possible array of problems. If our attention converges on too narrow a definition of data security it is likely that a set of security measures could be selected which contain a smaller problem scope than would have other measures selected with the broader problem definition in mind.

Because there are six categories of undesirable things which can happen to data in addition to the loss of the ability to process it, and because the negative dollar impact of these things or their probability of occurrence, or both, may vary widely as a function of which data is being considered, experience has shown it to be desirable to look at the dollar impact of an event and its probability of occurrence in a rather fine-grained structure; that is, looking at the results of each bad thing happening to every file or dataset.

The selection of appropriate security measures is highly dependent upon the specific problem to be contained. If our problem structure is too coarse, combining, for example, the consequences of both accidental and intentional things, the results will not usually provide the desired guidance to select a set of cost-effective protective measures.

Refer now to the format of the sample work sheet. The far left column is for listing an inventory of the data. It is suggested that these files be aggregated by system, such as "Life Beneficiary Pay", "Inventory Control, Sub Assy", or "Personnel Data, Non-Exempt Emp.", because they are most conveniently inventoried this way and are always most conveniently considered for risk assessment in the context in which they are used. "System" is used here to describe a major application area, as implied by the examples, and does not imply a physical facility.

Some files are used to support more than one system. In such cases, it may be more convenient to list them with each system in which they are used, and note in the Comments column that they

have been so listed. It is not safe to list only once those files which are used to support several systems because the system with which they are included may be the one less dependent on that file than might other systems be.

The first objective is to assign values for impact and probability for each intersection in the matrix. Many intersections describe problems which are sufficiently small that they may be neglected. Ordinarily, if the sum of v and p , as described in Figure 2, is less than 6, then it can be neglected. In some cases it is acceptable to set the threshold higher, but caution must be used. There may be security measures which will contain a large number of low cost problems but which cannot be cost-justified unless these small problems are identified. Care must be taken to avoid disregarding an intersection because only the per-instance dollar impact is low; it may well be that the probability of occurrence is sufficiently high to yield a high annual cost for this problem. If the cost of a particular data entry error is only \$10, this should not be ignored as too small to be important until it is also known that it does not happen many times per day.

There is a strong tendency to attempt impact and probability assessments far more exact than are actually required. This contributes materially to the time required to complete a risk assessment, without a corresponding increase in the value of the product. It is not uncommon when working with a group engaged in a risk analysis to find the discussion bogged down on the question of whether there is, in a particular instance, a \$115,000 or a \$132,000 problem when, in fact, it makes no difference which is chosen.

It is better to do the risk assessment making very gross estimates of both impact and probabilities, and then refine specific items later only if it is found that a decision to pursue a particular course requires greater precision. For this reason, an artifice is proposed to induce the risk analysis team to be sufficiently inexact, at least on the initial pass, to complete the job in a reasonable time. The use of factors of 10 (orders of magnitude) for both dollar impact and probability is recommended.

The justification for the seemingly complex formula for computing exposure in dollars per year lies in avoiding fractional exponents. The flexibility to work with high probability events in days and low probability events in years is provided. The sole value of the formula lies here. It is not a means of introducing an empirical weighting factor. Careful examination of the formula will reveal this. The use of either the formula in Figure 3 or the matrix on that page will yield the same result. In either case, all three values (v , p , and E) should be entered in the matrix. Its quite difficult to reconstruct the basis for a particular E if the v and p are no longer available.

It must be understood that the assignment of probabilities to specific human behavior problems in this area cannot be done from a sound statistical base. This should not seriously inhibit the risk analysis. With on-going systems with which there is body of experience, particularly as it applies to high-probability errors and omissions problems, the task is relatively easy. There is usually an experience base from which the team can work. It is usually more difficult to assign probabilities to dishonest behavior problems. Nevertheless, with the proposed gross quantification intervals, it has not been found too difficult.

Even if all white collar crime were reported to law enforcement agencies, (as opposed to the estimated 10-15% of detected instances) there would still not be a statistical base which would provide data better than informed judgment based on a thorough knowledge of the environment under consideration. People are far too complex to permit a statistically-based behavior analysis as it relates to the probability of members of groups committing specific crimes. In fact, if all the people in the United States who are users of data processing systems were simple gas molecules in a teacup, there would not be enough of them to obey the basic pressure/volume/temperature relationships of the gas laws. It is clear that the behavior of people, with their near-infinite complexity, will not yield to a rigorous, statistically-based, behavior prediction.

Common sense is a very powerful weapon in attacking a probability analysis. In a life insurance beneficiary payment system where several hundred to a thousand or more people know that it is relatively easy to change beneficiary address without risk of anyone verifying that new address, there is an exposure to at least one dishonest person successfully diverting checks to an address or mailbox from which he can get and then cash the checks. Such a situation should yield a probability much higher than once in 30 years, probably much lower than every ten days and so, using our exponential scale, we are discussing either once every 1000 days or 100 days. The selection of the more appropriate one of these two depends on several factors, including the general climate in which the system functions. If the number of people who know of the potential exposure is in the order of one to two hundred, it is perhaps reasonable to work with the 3 year, or 1000 days, probability. If the number of such people is in the thousands or if employee dishonesty is a sustained problem, then the 100 day approximation is probably better. This selection is left to the risk analysis team. However, the team must consider the general environment. If employee dishonesty is relatively rampant and accepted by management so long as it does not exceed established bounds, then a much higher probability of loss must be anticipated than would otherwise be the case.

It is quite commonly stated that there is no justification for an attempt to identify a back-up facility because no one else can possibly spare the machine time necessary to replace the whole

capability of the system which is down or which was lost in some fire or other catastrophe. The flaw in this rationale is the assumption that it is necessary to find a facility which can replace all of the capability that was lost. It is generally true that only 10% to 15% of the work is so critical to the organization that it cannot be deferred for three or four days without catastrophic impact. It is important that this 10% to 15% be identified, and that contingency plans be laid which include the availability of all of the things necessary to process elsewhere: including forms, programs, communications, data and people-in the event of a loss of the regular facility.

The time intervals which should be on the form vary with the nature of the organization under consideration. The intervals shown are more appropriate to large scale commercial banking, for example, than they are to fire and casualty insurance companies. Once these time dependencies are well understood, the data processing manager will usually find that the amount of processing required and the cost of an inability to process after loss of his facility makes an arrangement with other facilities for back-up not only feasible, but highly desirable.

4.0 HELPFUL HINTS

It is important that proper weight be given to the impact of errors and omissions. Data is more often destroyed or otherwise rendered useless, or even harmful, by people making mistakes than through dishonesty or malice. People whose loyalty and honesty are unquestioned, but whose judgment and competence leave much to be desired, are our greater enemies. Data security considerations must not be limited to concern for the acts of dishonest people. Otherwise, it is very difficult to achieve proper cost justification of appropriate security measures. Weigh all potential security problems.

It is of utmost importance when considering the potential for damage by dishonest or malicious people to keep mind that the vast majority of all white collar crime is committed by employees, not outsiders.

Most of the losses to dishonest employees occur when employees misuse system resources to which they are authorized access to get their jobs done. The people who steal from Accounts Payable usually work there or are authorized to enter or modify these data. The people who steal from inventory through manipulation of the data processing facility most commonly work in Inventory Control. The people who work in Accounts Payable usually do not steal from inventory or payroll. This situation must be kept in mind when considering the exposures to data security problems. Most improprieties against property directly involving the data processing system are conducted by people who work in that portion of the business from which the theft occurred, and by people who are very familiar with that particular functional area.

It is usually best to eliminate perceived individual personal integrity when performing a risk analysis. While the probability that an individual will engage in dishonest conduct clearly varies widely from person to person and clearly influences the exposure to problems originating in this manner, the factors which influence this individual integrity are not easily perceptible. Further, individual personal integrity is not a constant. It varies dramatically with time and with personal situations of which a risk evaluation team may be totally unaware. Satisfaction of personal pride, frequently reflected in care and precision in the conduct of a job, an admirable trait, can also lead to other endeavors to satisfy this pride. Conflicts between two ethics, for example, the need to pay for an urgently needed operation on a child and a desire to be honest, can be resolved in a manner not favorable to the employer. The highly motivated employee who feels passed-by on promotions may decide to get his increased income in a manner of his own

choosing. For these reasons, it seems most satisfactory to eliminate individual personal integrity as a factor in the risk assessment.

Most people in a position to engage in white collar crime are deterred when the potential for reward from dishonest conduct is limited to the absolute minimum necessary to the conduct of the job to which he is assigned. They are deterred by reasonable assurance of detection if they do something wrong. This is to say that people are primarily deterred by limits on the value to them of their dishonest activities, by the fear of being caught and, to a lesser extent, by fear of punishment.

The loss of the physical facility itself should be treated independently of the matter of loss of processing capability. It is misleading to consider the loss of processing capability as part of the cost of a loss of the physical facility. The loss of the physical facility in a properly planned operation may not result in a loss of all processing ability, and the loss of all processing ability need not involve the loss of the physical facility. There may well be other facilities on which the more critical data processing functions can be continued until the prime system is replaced with the result that the cost of the loss of the facility is only modestly greater than the replacement cost of all that destroyed. For this reason, it is recommended that loss of the ability to process be treated as a data security problem and taken into account when considering the impact of other problems on specific files.

When considering the problem of fire, bear in mind that fire can deprive the facility owner of services without destroying or in any way damaging the data processing complex itself. In high rise buildings, for example, severe fires on any floor below the facility, and, frequently, on any floor above, will disable that facility by depriving it of power, air conditioning, communications or elevators. Fire which destroys the supply of pre-printed paper forms can seriously inconvenience the operations and effectively cripple any function totally dependent upon those forms. It may well take longer to replace a destroyed supply of customized forms than it does to replace the hardware facility. It is necessary, to consider all aspects of each possible loss to fire.

It is important that data security and physical security definitions do not become confused. Data security problems are those which are contained by security measures in data processing hardware and software, and physical security problems are not just those which are contained by physical measures such as fire detection and quenching facilities. These interpretations do not yield a usable distinction and should be avoided.

5.0 THE RISK ANALYSIS TEAM

The composition of the team to perform the risk assessment is particularly critical to its success. The task cannot be done both quickly and well. It takes time. With even the best teams and a near optimum situation, experience has shown that the time required is about one month for each 2000 data sets or files considered. That figure is predicated on the assumption that the team is configured as suggested here and devotes the recommended amount of time to the task. Some experienced teams have reported an average rate as low as a file every 15 minutes of actual evaluation time.

The proper consideration of the impact and probabilities required to complete the recommended procedure requires the assignment of well-informed, properly motivated people. This job cannot be delegated to clerks as a routine task. Because it takes good people and, in a large shop, quite a while, it is suggested that the best way to convene and risk analysis is to agree that the people working on it will be required for only a half day per day with the other half spent at their normal duties. The alternative to this mode of operation, the full-time task force approach, seems to provide only a fast wind-up with a quick fade before a significant amount of work is completed.

The participants on the risk assessment team must include competent, senior representation from each of the following:

1. EDP operations management.
2. The department supported by or owning the data under consideration at the time.
3. The programmers responsible for support of that department, operation or function currently under consideration.
4. System programming, if the installation is large enough to have this as a separate function.
5. The internal audit function.
6. The department responsible for physical security. While these people may not be able to contribute a significant amount initially, their involvement usually results in their education in a way that may not be achievable by any other means.

In addition to the above, a strong senior management commitment to risk assessment is essential to its success. No amount of lower level concern will be truly effective unless everyone who

has a role in achieving security believes that more senior management has sufficient commitment to this area. It is often difficult to convince senior management that they should be concerned without a quantitative expression of the problems as might be derived from the risk assessment. This situation leads to a chicken and egg problem. There is a need of senior management support to get a properly manned risk analysis team organized, but management may not be sufficiently concerned about data security until it sees the product of their labor.

6.0 AN EXAMPLE

We have chosen a hypothetical payroll operation to demonstrate how the risk assessment process might work. A payroll system was selected because it offers a wide variety of data security concerns, including the potential privacy problems associated with unauthorized disclosure.

The particular payroll process described is probably not the best way of running any specific payroll system. It has been tailored to provide a convenient example, but nothing has been done to make it more or less amenable to the risk assessment procedure described in this paper.

The payroll process which we examine here has four stages, as shown in Figures 4 through 7. The four stages are these:

- Stage 1: Maintenance of tables and master files to accommodate variations in individual employee status and variations in tax rates, stock prices, and such data.
- Stage 2: Verification, through the application of validity criteria, of the probable correctness of transaction data as input to payroll calculations.
- Stage 3: Payroll calculations which yield output orders for the issuance of checks, statements, updated master files, etc.
- Stage 4: Preparation of output documents, reports, and cumulative payroll data.

In our example, we assume the following:

1. The operation is in the private sector. This assumption is made so that we can include the need for privacy of individual pay records which need is more common to the private sector than to government institutions.
2. The employer is a manufacturing concern paying 12,500 people. It is a relatively mature firm. Each functional area, such as inventory control, accounts payable and receivable, transportation, and payroll, is well-defined. These functional areas all utilize the data processing center for support. EDP is a cost center.
3. The internal audit staff has no EDP professionals and so has no means of effectively examining machineable records, nor can it critically examine program documentation.

4. The programming staff reports to the EDP functional manager. Programming, like all other EDP, is a cost center.
5. There is no history of dishonest conduct on the part of any professionals in the EDP area.
6. Petty pilferage from inventory has been a problem for many years. Some employees have been discharged for particularly blatant pilferage, but no cases have been referred to law enforcement agencies.
7. About once a year, a relatively junior clerical employee has been discharged after being detected in some sort of embezzlement. No cases of dishonesty have ever been referred for criminal prosecution.
8. The business environment is highly competitive with proprietary product designs and sales information fairly commonly lost to competitors through their hiring of key people.
9. The management has not tolerated detectable abuses of expense accounts. The proper reporting of all expenses is expected and compliance is generally good.
10. All employees recognize a strong management belief that dishonesty, particularly in exempt employees, should not be tolerated.
11. A high error rate in input data from all areas has long been tolerated. No strong drive to improve the integrity of information has ever been made. There is a general low level of confidence in the accuracy of all business data.
12. Payroll is run weekly on second shift on Friday night as a local batch operation done with people from the Payroll department in attendance but not operating the system. Check forms, completed checks, and all printed materials stay in possession of the Payroll people. All payroll tapes and packs are kept in the local tape library but are locked in a separate cabinet to which Payroll people keep the key. Payroll people do not know about scratch tapes and spooled output, and no one wants to complicate things by telling them.
13. A copy of each of the important files modified in any day is made each night and sent to a vault in a separate building. Payroll data are not segregated in the off-site vault.
14. The system is a 370/145 running VS-1. It is a 7-day, 3-shift operation.
15. The 370/145 is installed on the second, top, floor of the corporate headquarters. A dry pipe sprinkler system is

installed in the machine room. The pipes are not charged until two products-of-combustion detectors have indicated a possible fire. Water will discharge only from those heads exposed to the heat of the fire. No fire detection or quenching system is on the floor below nor in any space around the machine room. Hand extinguishers are available in the machine room and in surrounding spaces. Pre-printed forms and other paper supplies are in the basement. Check paper for payroll is in a Payroll Department locker not well protected against fire or theft. Lead time on replacement check forms is 3 to 4 weeks.

16. Actuarial data indicate that a complete destruction of the building from all causes, including fire, civil unrest, falling aircraft, and windstorm, can occur with a probability of once in 450 years. There is no meaningful flooding threat but the building roof is a constant annoyance with its tendency to leak and the machine room is immediately under the roof.
17. The power company reliability has been good, but the facilities are heavily loaded. Brown-outs are becoming common in summer as a result of a need to share power with other companies in the net. No back-up power and no UPS is provided.
18. No arrangements have been made for back-up of critical work at other facilities.

The work sheet shown in Figure 8 has listed in its leftmost column the fourteen data sets comprising our hypothetical payroll system. The immediate task is to assess the impact and probability of losses to these. We can simplify the task by identifying those data sets for which we know that disclosure of content cannot represent a significant problem. These include, as examples, the payroll data tables (PAYMASDATA), which contain no individual employee data and PAYNAMADD.

Consider at PAYMASDATA, the tabular data to support payroll calculations. It may be expected that greater than usual care will be exercised in introducing changes to these tables. Further, it is reasonable to assume that only gross errors in these changes will be caught before these data are applied to payroll calculations. Minor errors will not be caught and will be reflected as errors in pay, which errors must be corrected at significant cost and embarrassment to the employer.

The history of errors and their general acceptance suggest that a possibility of once in 3 years is not unreasonably high. Thus, we assign a "p" value of 3 to the probability of accidental modification.

The dollar cost of an error in pay rates or tax rates, which is not detected until after a payroll cycle is completed, when some

weighting for embarrassment is applied, cannot be as great as \$100,000 nor smaller than \$10,000, and is probably closer to the \$10,000 figure. On this basis, use a "v" of 4. We can see that there is a potential exposure of \$3.3K/year. However, all of the exposures to errors of this type must be examined to get an assessment adequate to support any decisions on appropriate corrective measures.

Accidental destruction of PAYMASDATA costs are limited to those necessary to produce a copy from the back-up copy in the vault. If no copy was available, a fairly unlikely situation, the cost of reconstituting the file is still small.

It is highly improbable that dishonest persons would select the rate tables as a means of rewarding themselves, but a dissident employee bent on creating embarrassment might. The figures reflect that.

There is strong belief in our hypothetical company that payroll information should be held in strict confidence. Because the company is one of the largest employers in the area, many merchants, automobile dealers, and others would like the payroll listing. Because these listings are generated for the personnel department and others, and because no real controls exist over their distribution nor are there procedures for individual accountability, there is a real possibility of these listings accidentally or intentionally getting to those outside the company who might want them. The accidental and intentional disclosure columns reflect this. Further, because of the strong feelings about privacy, it is difficult to imagine an impact measured in lost morale, general dissatisfaction, and such, to be less than \$100,000.

The rest of the form was completed by simply reviewing the impact and probability of each occurrence with the risk assessment team and recording the figures yielding the closest approach to a consensus.

The impact and probability of a loss of processing facility as a function of time has been done, not by data sets, but by functions (stages) within the payroll operation.

RISK ANALYSIS WORK SHEET

SYSTEM/ DATA SET NAME	ACCIDENTAL			INTENTIONAL			Exposure if Unable to Process for:					COMMENTS	
	Disclosure	Modification	Destruction	Disclosure	Modification	Destruction	HOURS						
							2	4	8	12	18		
					Ed v								

Where:

v is a function of dollar impact, as shown in Figure 2,

p is a function of the estimated frequency of occurrence of the event, as shown in Figure 2,

E, a function of p and v, is the estimated loss in dollars per year from that event (vertical column) impacting that data set (horizontal row), calculated as shown in Figure 3 or from table in that figure.

Figure 1

If the dollar impact of the event (vertical column) on the data set (horizontal row) is:

\$ 10, let	$v = 1$
100, let	$v = 2$
1,000, let	$v = 3$
10,000, let	$v = 4$
100,000, let	$v = 5$
1,000,000, let	$v = 6$
\$10,000,000, let	$v = 7$

If the estimated frequency of occurrence is:

Once in 300 years, let	$p = 1$
Once in 30 years, let	$p = 2$
Once in 3 years, let	$p = 3$
Once in 100 days, let	$p = 4$
Once in 10 days, let	$p = 5$
1 per day, let	$p = 6$
10 times per day, let	$p = 7$
100 times per day, let	$p = 8$

Selection of values of v and p

Figure 2

PAGE 25

Method 1: $E_{\$/yr} = \frac{10^{(p+v-3)}}{3}$

Method 2: Values of p

	1	2	3	4	5	6	7	8
1					\$300	\$3K	\$30K	\$300K
2				\$300	3K	30K	300K	3M
3			\$300	3K	30K	300K	3M	30M
4		\$300	3K	30K	300K	3M	30M	300M
5	\$300	3K	30K	300K	3M	30M	300M	
6	3K	30K	300K	3M	30M	300M		
7	30K	300K	3M	30M	300M			

Values of $E_{\$/year}$

Determination of Annualized Risk, E.

Figure 3

PAGE 26

Payroll Stage 1 - Update

<u>Input</u>	<u>Process</u>	
o Payroll Data (1) (PAYMASDATA) ^x	- Verify changes - Apply changes to masters - Duplicate masters	o Payroll Data (2)
o Personnel Master (1) (PAYPERSMAS) ^{xx}		o Personnel Master (2)
o Bond Deduction Master (1) (PAYBONDUC)		o Bond Deduction Master (2)
o Other Master Data (1) (PAYNAMADD) ^{xxx}		o Other Master Data (2) o Error Listings (PAYMASERR)
o Changes To: Payroll Data (PAYDATCHG) Personnel Mas. (PAYPERCHG) Bond Deduc. (PAYBONCHG) Other Mast. (PAYNAMADD)		o Back-up Dataset copies

x Tables of changeable payroll data not specific to employee, such as tax rates, hourly rates, etc.

xx Records for each employee, rate, deductions, garnishments, etc.

xxx Payroll data, not employee-specific, such as names and addresses of recipients of deductions, attachments, etc.

Figure 4

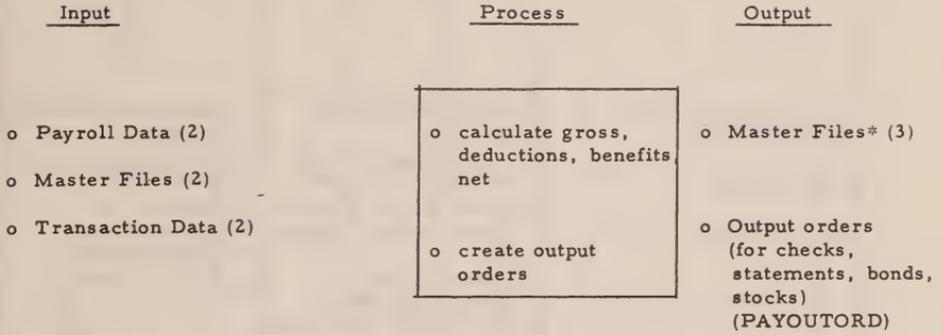
Payroll Stage 2 - Verify

<u>Input</u>	<u>Process</u>	<u>Output</u>
<ul style="list-style-type: none">o Transaction Data (1)<ul style="list-style-type: none">- clock card (PAYCLKDATA)- local mileage and overtime meals (PAYMILDATA)o Payroll Data (2)o Personnel Master (2)o Bond Master (2)o Other Master (2)	<div style="border: 1px solid black; padding: 5px;"><ul style="list-style-type: none">o check format, contento edit, reformat, sort, etc.</div>	<ul style="list-style-type: none">o Error lists, Rejects (PAYTRANERR)o Transaction Data (2)

Figure 5

PAGE 28

Payroll Stage 3 - Calculate Payroll



* Cumulative data in master files

Figure 6

Payroll Stage 4 - Output Documents and Reports

- | | | |
|---|--|---|
| <ul style="list-style-type: none"> o Cumulative Payroll Data (1)
(PAYCUMDATA) o Output orders o Master Files (3) | <ul style="list-style-type: none"> o Update cumulative accounts o Accumulate deposits to banks, amounts to credit unions, garnishments, taxes, benefits, etc. o create checks o create statements o cumulative labor stats. | <ul style="list-style-type: none"> o Cumulative Payroll (2) o Checks o Statements o Bond P.O.'s o Reports, etc o Tapes to banks o Tapes to feds o Tapes to states |
|---|--|---|

Figure 7

PAGE 30

7.0 CONSIDERATIONS IN THE SELECTION OF SECURITY MEASURES

CONSIDERATIONS IN THE SELECTION OF SECURITY MEASURES.

INTRODUCTION: This section has been included to provide general guidelines for the consideration of candidate security measures. It is anticipated that appropriate measures will be evaluated and selected only after a detailed assessment of the potential cost which these measures will displace. The cost justification for any measure or combination of measures must be that the problems which the measures will obviate would cost meaningfully more than the corresponding security measures.

An array of security measures is detailed in the following paragraphs. The intent is to familiarize readers with the protective measures that should be considered for inclusion in systems, how these features integrate into a coherent, consistent mechanism, why they are needed and how they might be used.

The primary classes of hardware and software protection measures support:

- Positive unique identification of people, devices and other named system resources.
- Authorization of system activities involving interactions among people, data, programs, devices and other named system resources.
- Surveillance of system activity-including means of achieving strict personal accountability of people for their actions.
- System integrity-including means of achieving hardware and software integrity, physical security and protection against wiretapping and electronic and acoustic eavesdropping.

Coherence and consistency at the system level of the security measure complement are not the only major concerns faced by those who must select security measures. Other critical criteria of adequacy are:

- Performance.
- Optionality of functions.
- Recoverability.
- Testability.
- Considerations of the effects of maintenance, servicing, and

distributed intelligence architectures on the protection mechanisms.

These security features should become part of a broad security plan formulated and implemented by the system administrator that enables him adequately to protect his data assets from accidental or unauthorized intentional disclosure, modification and destruction.

To achieve adequate protection, installation management should try to:

- Bestow the least capability necessary to enable users to get their work done, and ensure that it is difficult for them to defeat constraints or to misuse authorized capabilities.
- Hold each user personally accountable for his activities on the system.
- Impose a high actual and perceived risk of apprehension and significant penalty for users' misuse of the system.
- Identify and reduce the incidence and impact of errors and omissions attributable to people in the data processing environment.

In other words, security features should help the system owner to institute and enforce prudent protection, and they should be such that, in the event of wrongdoing, unquestionable evidence of the nature of the activity and the identity of the wrongdoer is available.

Given the above, the governing broad objectives for the selection of any set of security measures in any system are:

1. Security features should enable installation management to hold each user personally accountable for his activities on the system.
2. Security features should enable installation management to grant to each system user only the least capability necessary for that user to accomplish the work he is required to do.
3. Security features should make it demonstrably difficult for a system user to misuse without risking detection a capability that he is authorized to have, or to defeat any mechanism that is intended to deny him a capability that he is not authorized to have.
4. Security features should support installation management's efforts to create a high actual and perceived risk of apprehension should any user attempt to misuse a capability that he is authorized to have or to use a capability that he

is not authorized to have.

5. Security features should be useful in identifying and in reducing the frequency and the cost of errors and omissions on the part of system users.
6. Security features should be useful in protecting not only against normally high-exposure threats but also against normally low-exposure threats that may be highly significant in a particular environment, industry, or installation.
7. Security features should be designed such that their positive contributions in terms of asset protection and increased manageability, predictability, reliability, and imperturbability of the system can be seen to outweigh any unavoidable negative impacts such as performance degradation and human inconvenience.

Identification:

Personal Identification: Positive unique identification of people using the system is clearly a requirement if authorization and surveillance mechanisms are to be of value. Personal accountability and "least-privilege" authorization mechanisms are necessary for addressing an estimated 70% of data processing-related losses occurring today.

Holding a person accountable for his actions and enabling him (in realtime) to engage in only certain activities within the system requires knowing, with high certainty, that he in fact is who he says he is. Another consideration is that the activity record, or journal, must be admissible and defensible evidence; it should be so strong as to withstand attacks upon its credibility.

A personal identification process has two parts:

1. Identification.
2. Verification.

Identification occurs when the user provides his identity; the "name" by which he is known to the system, which is unique to him and relatively unlikely to change, and which will be used during subsequent authorization and surveillance processing. Verification occurs when the individual, having provided an identifier, "proves" to the system, by passing some further test of identity, that he is in fact the person indicated by that identifier.

The state of the art today permits inexpensive verification by testing people for something they know (key-entered passwords) and for something they possess (magnetic stripe credit cards). The first method is commonly used, very inexpensive, and relatively frail; passwords may wittingly or unwittingly be given away without noticeable effects that would alert the user, management, or auditors. The second method, use of magnetic stripe cards, is available but not so widely used. It is little more expensive than passwords, and is much stronger, particularly when implemented as recommended below.

A third method of verification involves testing for something the person is; a personal, unique, and stable characteristic such as voiceprint, fingerprint, hand geometry, or signature dynamics. These areas have been researched with some success, but to date no sufficiently inexpensive and reliable technologies have come into general use.

System design must also take into account the need to protect the identification mechanism itself, including the tables, profiles, other data, and software routines.

Some secure method must be available for identification and

verification of individuals submitting batch jobs, either locally or at remote job entry sites. This should include provision for the user ID on a control card and the verifier either on the same card or on another card that may be located randomly elsewhere in the deck. At most installations, the single-card approach is considered secure enough; where the job-entry site is attended the attendant can visually identify the individual submitting the job and also check the verifier on the control card against a list of correct verifiers, and accept the job deck only if the correct verifier appears on the card. Where the job-entry site is unattended, the user should himself protect the card containing his ID and verifier; where the job-entry site is a "mail drop", or courier pickup/deliver station, the drop should be physically protected or the procedure changed.

An installation option, where passwords are required or optional, the user should be able at will to alter his key-entered verifier (password), or be required to alter it at specified intervals. Also, at installation option, management should be able to require the use of installation-issued passwords. These should not be alterable by the user himself.

The identification mechanism must uniformly support print/display inhibit of identifiers and verifiers where the feature exists in hardware; otherwise, for printing terminals, the mechanism should provide a backspace/overstrike field for entry of the sensitive data as a means of concealing the data.

The identification mechanism should support terminal disconnect or lockup after an installation-specified number of unsuccessful identification sequences. This hinders casual attempts to masquerade and introduces an unacceptable delay factor into more sophisticated attempts to gain access, such as through use of some programmable device masquerading as a simple keyboard and simply transmitting all possible password combinations.

The identification mechanism should provide, at installation option, a LOGON message providing a sequence number ("your nth logon") or data/time last logged on, or both, with data/time preferred if only one can be provided in design. This enables the proper user to detect successful masquerade under his identity.

Another important capability that should be considered is a reverification sequence (required re-entry of the verifier) that could be invoked at installation option. This would enable system determination that the proper person is still present at the terminal after some specified period of line inactivity; for example, prior to accepting terminal input after a prolonged apparent "think time" delay, or prior to transmitting output to the terminal after lengthy transaction processing. If the proper verifier is not entered upon demand, the process should be gracefully suspended so that the proper user can resume his work at the indicated point.

Personal Identification Summary:

1. A personal identification function is a firm requirement for all systems and subsystems that employ authorization or surveillance mechanisms.
2. The personal identification mechanism must yield positive unique identification of individuals using the system, such that subsequent authorization and surveillance activities, which are based on the personal identifier alone, can be shown to be using identifiers that represent the correct individuals with a degree of confidence adequate to the particular security situation.
3. The personal identification mechanism should include a verification process that yields a high degree of certainty that the person presenting an identifier to gain entry to the system is in fact the individual properly represented by that identifier.
4. For terminal operations, verifiers of personal identification should be print/display inhibited.
5. For batch operations, the identification mechanism should provide some secure means whereby users can provide personal identification accompanying their jobs.
6. For terminal operations, the identification mechanism should provide for a reverification sequence prior to initiating or accepting transmissions after a specified period of inactivity on the line.
7. The identification mechanism should be such that even in distributed intelligence configurations, where more than one identification process exists, the collective effect of all is that management can reconstruct for any journalled activity or event which individual user was associated with it.
8. The identification mechanism should enable installation management to specify, when key-entry verifiers (passwords) are required, that users may alter their passwords at will, or that users must change their passwords at specified intervals. Management should be able also to require the use of passwords that are assigned, distributed, and changed by installation management, and cannot be altered by the users.
9. To the extent economically feasible, the tables, profiles, other data, and software routines associated with the identification mechanism should be shown to be protected against unauthorized access or undetected tampering.
10. The identification mechanism should be able to accept as an

identifier, at installation option, either a key-entered name or a magnetic stripe card character string (although this latter personal identification procedure, as opposed to authentication, is not recommended for most applications).

11. The identification mechanism should provide for terminal lockup or disconnect after an installation-specified number of unsuccessful identification attempts.
12. The identification mechanism should offer, at installation option, a LOGON message providing a sequence number or date/time last logged-on, or both.

Device Identification: Positive unique identification of devices within the system is fundamental to the integrity of operations and may be a firm requirement for systems employing authorization and surveillance mechanisms. This capability enables detection of and recovery from switched-network line problems, some limited defense against intruding alien devices, control over certain interactions (a form of authorization), and enhanced surveillance activity.

Device identification can be accomplished in several ways. Dial-up terminals, certain controllers, and some CPUs today offer a "hard-wired" factory-set identifier that is transmitted automatically by the device upon command from an attached device. On non-switched multipoint networks, or with local attachment, adequate identification is provided by the address at which a device is polled or selected (although a security exposure exists where it is trivial to swap cable connections at the controller either accidentally or intentionally but without detection).

These methods are satisfactory for local identification of devices, but they are not necessarily satisfactory for higher-level authorization or surveillance functions unless each such unique identifier is mapped to a system-unique name for the device, which name is operated upon by the higher-level mechanisms. As an example, a subsystem controller may itself use station IDs in communicating with its terminals, and its own ID in communicating with the central processor. The only journaling mechanism is informed by the subsystem controller, with each message, which terminal stimulated the message. In most such cases the intelligent controller itself can contain an authorization and/or a surveillance mechanism sufficient for its own needs. The information acted upon by the authorization and surveillance mechanisms, and the collective record of transmissions provided by the surveillance mechanisms, would not be incomplete or ambiguous.

Many communications devices that accept dial-up connections are today equipped with "potential disconnect", or line-break sensing equipment, and are capable with proper software support of initiating device ID reverification procedures when a potential disconnect condition exists (as when line noise or transients have occurred). Communications systems design should include support for this equipment, such that when the potential disconnect interrupt is raised the system response will be verification that the expected device is still present on the line. If the device is present, the session should continue without interruption, even with no indication to the user. If the expected device is not present on the line, the system should gracefully suspend the session if possible, for future resumption by the user with no loss of work already accomplished during the interrupted session.

If the potential disconnect sensing equipment is present but the terminal involved is not equipped with device ID, the

reverification sequence should instead verify that the expected user is present on the line; otherwise, the reverification sequence should be the same as described above. Note that this implies that the active communications process must retain the device and/or personal identifiers related to the active sessions for possible use as comparands during such reverification sequences.

Good operations practice, as well as hardware integrity considerations, make most desirable the individual identification of portable media such as disk packs, tape reels, cartridges, floppy disks, and so on. This capability can be used to reduce or eliminate significant sources of lost data and processing time, such as operator mismounts, incorrect volume specification, and a number of integrity flaws that are described in the integrity section.

Device Identification Summary:

1. Means of identifying hardware devices within the system is a requirement for all systems and subsystems that employ authorization or surveillance mechanisms or attempt to achieve high integrity.
2. The device identification mechanisms should yield positive identification of individual devices interacting with the system, such that authorization and surveillance mechanisms elsewhere in the system can be shown to be operating upon, and creating activity records employing, unquestionable correct and unique device identifiers.
3. Devices that interact with other devices through the switched network should provide a unique identifier feature that transmits the identifier from the connected device to the requesting device.
4. In all other cases, the device identification mechanism should be such that it can be shown that authorization and surveillance mechanisms (which may be several), and may be distributed among hardware and software subsystems and connected systems) collectively and logically are operating upon unique identifiers and are keeping activity records that can be used to reconstruct the unique identities of involved devices.
5. Wherever possible, portable media should be uniquely and positively self-identifying. Where appropriate, this self-identifying capability should be used in conjunction with sensing of "not-ready to ready" status transitions of storage devices employing removable media, to detect and recover from improper media substitutions.

Software and Data Object Identification: Positive unique identification of named software and data objects is important to system integrity and to authorization and surveillance mechanisms. The possibility of accidental or intentional unauthorized substitution of one object for another with the same name is tantamount to uncontrolled modification of the original object, can be more dangerous in certain situations, and reflects a serious system design flaw.

Also a serious flaw is the possibility of reproducing an object under a different name such that the system "loses track", cannot associate the replica with the original, and therefore, cannot give the same protection to the copy as to the original. In systems where this can occur, the only defense is a well-operated journalling procedure, which, of course, is deterrent, not preventive.

1. Positive unique identification of all named software and data objects, whether system, subsystem, or application, is an important requirement for systems that attempt to achieve high integrity or that employ significant authorization or surveillance mechanisms.
2. System design should be such that truly identically-named objects cannot coexist in the system.
3. System design must preclude unauthorized and undetected substitution of objects and of object names, and must preclude unauthorized, undetected, and untraceable replication and renaming of objects.
4. The system must automatically provide identical protection to all copies of an object (under any name) as is provided for the original. This may be accomplished through addressability structures, object-name mapping, symbol resolution mechanisms, surveillance mechanisms, or by other means, but it is a basic integrity requirement.

Authorization: Authorization (often called access control) is the capability that enables installation management to establish which interactions among system elements (including people and named resources) are allowed. Among other things, it provides a means of constraining people to do only those things that management wants them to do, denying them the ability to do things that management does not want them to do.

An authorization mechanism should, to the degree needed and specified by installation management:

- enable only authorized users
- to perform only those functions which they are authorized to perform
- upon only those data to which they are authorized access
- using only those hardware and software resources which they are authorized to use.

In general, the principle of "least privilege" should govern and the authorization mechanism should support this by providing the means of controlling as many resources as possible. The less a person using the system is allowed to do (consistent with the work he is required to do), the safer will be the system's other users, and the individual's own processes and resources.

The authorization mechanism generally should operate upon names of elements and should be invoked when one named element refers to another, for example by requesting access, calling for execution, or requesting a system service. The mechanism should be invoked at the point where the controlling process resolves such symbolic references.

Named elements which are candidates for authorization control include:

- Persons.
- Devices (terminals, controllers, printers, CPUs, etc.).
- Data objects (data sets, segments, libraries, records, etc.).
- Executable objects (transactions, commands, programs, etc.).
- Storage media (cartridges, reels, packs, etc.).
- System control objects.
- Application subsystems (both software and hardware).

- Named groups of these elements.

The authorization mechanism should prevent or allow interactions among these elements based not only upon the names of participant elements but also upon the nature of the requested interaction (for example: requests to create, read, alter, append data to, delete or destroy a data object), upon the nature of the participant elements (for example: sensitive data must be displayed/printed at only designated output devices), and upon testable external conditions (for example: time of day, date, storage space available to the user, other people or processes currently active, and so on).

Installation management should be able to specify the extent to which authorization for certain kinds of interactions implies that the holder is authorized for other kinds of interactions. For example, it should be installation management's, not the designer's, decision that "create" authority includes "alter" authority for a data object. The authorization mechanism should not force such hierarchies of authority upon management.

Installation management should be able to specify the extent to which certain authorities held by a user imply his ability to bestow given authorities upon other users. For example, a person's authority to alter a data object should only at installation option imply that he can authorize others to interact in any way with that object. In general, the three authority levels of:

1. Ability to interact,
2. Ability to authorize interactions,
3. Ability to appoint those who may authorize interactions,

should be distinct independent conditions. None should, except at installation option, imply either of the others. This is analogous to the distinctly different authorities involved in entering a bank vault, guarding the vault (deciding who may enter), and appointing guards.

The authorization mechanism is driven by a structure of authorization data, or "rules". This is in a sense a model of the activities that management expects and considers desirable within the system. It is important that the authorization data be correct and adequately secure, because it actually controls system activity and has great potential for disruption.

It should be very simple for management to establish, modify, delete, and display the authorization data. If these processes are complex or difficult or unwieldy, errors will be more likely, disruptions may be more frequent, and use of the authorization mechanism by installations will be less likely, and the important function afforded will be less useful, than would otherwise be

the case.

The authorization mechanism, to the extent feasible, should be self-protective such that erroneous, anomalous, or inconsistent authorization data entries are detected and reported as early as possible, hopefully at the time of entry and at least at the time they are first used in normal authorization checking.

In all likelihood, the authorization relationships within a given system will change frequently as people, data, software, and hardware change with time. The burden of keeping authorization data in line with real, current needs could easily grow out of hand (as can the amount of authorization data) if flexible entry, updating, and display capabilities are not provided. Since there may be significant effort involved in keeping the authorization data current and correct, management must be able to delegate this work as much as possible to administrators and to users themselves in the normal installation. It needs to be delegable for other reasons as well, the principal one of which is that supported departments; those whom the applications and data are serving, must be able to control access to their own resources. However, the capability of concentrating, or centralizing, this work is a requirement in certain environments.

Another argument for simple and flexible entry, modification, and display capabilities is that these in the past have been perceived by installations to enhance the manageability of the system (quite apart from any security enhancement, if good management and security are indeed separable), and where they have not been offered, management has been reluctant to use the authorization mechanism.

The authorization mechanism should ensure that management is protected against destructive or disruptive secondary effects of modifications to authorization data. Where an individual with authority to use an object, and to enable others to use the object (who in turn may enable still others to use the object) is about to have his authority removed, the consequences must be well understood. One consequence (depending upon design) might be that all users whose authority proceeds from that individual will lose their authority when his is removed; this may be acceptable in some cases, and it may be catastrophic in others. On the other hand, if the authorities proceeding from his authority are undisturbed (or untraceable) when his is removed, this too can be catastrophic, or at least create an administrative burden. The authorization mechanism should enable installation management to discern the ultimate effects of such removals or modifications of authority. This requires that the authorization data, including backchained or derivative authorities and all grouping relationships, be displayable.

It can be a traumatic process to transform an installation from one with little or no authorization control to one that is heavily controlled. At most installations, management simply

does not possess the required specific information to create the complete set of authorization data, and the information can be difficult and costly to collect. Thus, a gradual transition is indicated. Mechanisms have been proposed to aid this process. One such is to include in the authorization mechanism a capability such that checking based on the growing body of authorization "failures" cause denial of the requested interaction. Instead, the interaction is allowed to proceed and a record of the failure is kept for subsequent analysis. In this way, management can correct the expected high incidence of errors during the transition without disrupting normal operations. As confidence in the authorization data increases, the normal authorization failure processing can be used increasingly until the system has been converted.

Since damage to the authorization mechanism or data can disable operations, some bypass mechanism or procedure must be available so that management can decide whether to continue operations in an unprotected mode. Authorization mechanism design should not assume that management uniformly believes that system shutdown is preferable to interrupted or degraded protection. Any bypass mechanism is sensitive and dangerous and must be shown to be safe from unauthorized use.

The ability to create named groups of system elements that can share common authorization attributes is an important administrative tool. Such groups can be treated, from an authorization point of view, as elements themselves; this enables management to classify elements and thus reduce the number of individual entities with which it must deal on a frequent basis.

It should be possible to declare an element to be a member of more than one group, and to give specific elements that are members of a group additional or reduced capabilities relative to the group; this flexibility amounts to templating (or performing complex definitions automatically) and can reduce the administrative overhead significantly.

An authorization mechanism can make already difficult system back-up and recovery problems still more complicated. If all or a significant part of the system's operations must be brought up on another hardware configuration, perhaps one that must share its capacity with another, conceivably "hostile" workload, then the authorization structure should be such that the move to the new system is not inordinately difficult, requiring wholesale revision or piecemeal deletion of integrated authorization data. If great back-up/recovery difficulties are introduced as a result of the authorization mechanism, then a reluctance to employ the authorization mechanism at all, will inevitably evolve.

An authorization mechanism may provide installation management any appropriate subset of these functions or capabilities:

Summary of Authorization:

1. The means to grant to each system user only the least capability necessary for that user to accomplish the work he is required to do.
2. The ability to define for each named system element the minimum set of interactions permitted with other system elements consistent with accomplishing the work the system is intended to do.
3. The ability to include system conditions (such as time of day) as parameters of the authorization decision-making process.
4. The ability to distinguish among different kinds of capabilities (such as create, read, alter, and destroy objects, and the ability to authorize other users to do these) in establishing the authorization data.
5. A means of constructing named groups of elements of the same or different kinds, and of handling these groups as elements themselves.
6. The ability to specify which capabilities "automatically" include other capabilities (such as "alter" includes "read" authority, and "create" includes "authorize others to read").
7. A means of displaying in well-formatted form all or selected portions of the authorization data.
8. The means to convert gracefully from a no-authorization operation to one where authorization controls are heavily used.
9. A way to include a bypass capability as protection against system paralysis in the event that the authorization mechanism itself is damaged or disabled.
10. The ability to move all or part of the system operation to some back-up system in the event of disaster. Design must ensure that this is not made more difficult or impossible.
11. A self-checking capability such that logically erroneous, internally inconsistent, or anomalous authorization data is detected and reported to management either at the time of entry or at the first instance of attempted use during normal operation.
12. Protection against potentially disruptive or destructive secondary effects of modifications to the authorization data.

13. The means of setting (or allowing users to set) authorization "defaults" that would automatically be applied to resources individual users own.
14. The ability to control the amount of main storage space, the amount of external storage space, the number of external storage media (packs, cartridges, reels, etc.), and the amount of processing time made available to individual users.
15. Means specifically of controlling access to data records and fields within those records; this capability is growing in importance as more sophisticated products emerge, and organizations increasingly amalgamate their data collections while permitting growing numbers of people to share access to them.

Surveillance: Surveillance mechanisms are the means whereby installation management can designate certain events as "triggers" for specific reactions, can specify those reactions (which may include journaling the event), and can subsequently inspect the record of events.

The objective of the surveillance mechanism is to ensure that management can detect and react appropriately to activities that may constitute security threats. The surveillance mechanism must provide a means of achieving strict personal accountability of users for their actions on the system. In addition to such accountability processing, the surveillance mechanism may protect in real-time against damage from certain events, and should act as a strong deterrent to the user who might otherwise abuse his privileges but who perceives, because of the surveillance capability, that the risk of detection is unacceptably high.

The surveillance mechanism should support three major activities:

1. "Trigger-event" designation.
2. Designation of reactions to specified events.
3. Management inspection (post-processing) of the activity journal or journals.

The surveillance mechanism should first enable installation management to specify which events (such as LOGON, OPEN for write) and event characteristics (such as data sensitivities, numeric values of data fields) will trigger a surveillance reaction. Management should be able to make, alter, and display such specifications interactively, and easily.

In general, any event that can be designated as requiring an authorization test is a candidate surveillance stimulus. There should be no designed-in constraint that only an invoked authorization test can stimulate surveillance; the two activities should be independent such that an event can cause either or both.

The surveillance mechanism should provide for a number of optional surveillance reactions, depending on the nature of the detected event (an authorization-test failure, for example, as opposed to a success). Selectable reactions should include real-time alerts to management such as a warning bell and message to a designated console, suspension or termination of an offending process with a variety of messages to the user such as true messages, misleading messages, or no message, automatic invocation of special monitoring of an offending process if it is not suspended or terminated (such as complete journaling of associated system activities or interactive traffic), management-invoked real-time display at a designated console of the full interactive traffic of an offending terminal, and "normal" journaling (whose event records should include but not

be limited to such management-specified data as identifiers of all involved elements, the nature of the event, security data such as authorization status, time day, date, and so on).

The event journal itself is a major security asset; at times, it is the most important one. It must be protected from all but authorized access, and to the extent possible from destructive conditions such as power failure to a volatile store. It should be demonstrable that the journal and the journalling process are reasonably safe and cannot be subverted easily, at least without detection.

It should be noted that, under the Federal Rules of Evidence, computer output is admissible in both civil and criminal proceedings if it is determined to be:

1. A regularly-kept timely record.
2. Of regularly conducted business activity.
3. Whose preparation has been deemed "trustworthy" by the court.

The first two conditions are relatively easy to establish for a well-run enterprise; the third, may present a problem if it cannot be shown that the records and the record-keeping process itself are reasonably safe from accidental and unauthorized intentional interference. This showing is not only essential to the court's determination of admissibility, it is also an important defense against attacks upon the credibility of the output.

The journal post processing mechanism-the inspection function-should offer both interactive query and report generation functions. If management does not have this processing flexibility and power, the likelihood is that the journal will not be inspected regularly, users will come to know this and the deterrent value will be lost.

Both the interactive query and the report generation functions should support complex Boolean and arithmetic operations upon data names and numeric content. They should be able to perform such operations also upon derived statistical data about the journal contents; this would enable management analysis of patterns and departures from patterns of activity. It should be possible for management to specify that certain reports be automatically generated periodically.

The surveillance mechanism has more uses than just support of data security, and it need not exist only in that frame of reference. Accounting and recovery mechanisms and load-balancing, tuning, and education tools require some of these capabilities. A design may be such that one multi-purpose mechanism can accomplish all or most of these ends.

Because it is desirable to monitor system use to identify changes needed to improve efficiency of the work flow in and around the system, management would be expected to so employ an available surveillance mechanism. This can result indirectly in improved security of operations. If a system user is advised that management has detected a pattern of frequent errors in his conduct of certain activities and is offering help, there will be an induced awareness on the part of the user that his activities are being reviewed. In this way surveillance can be productively employed without the necessity of justifying it on the basis of detecting or inhibiting dishonesty on the part of the users.

The surveillance mechanism design must give due consideration to the problems of archiving extensive data for what may be prolonged periods, even years. The ability to easily off-load voluminous journal data, to condense it as much as possible, and to on-load easily the same data for inspection much later in time, perhaps on a different machine complex, is important. Such capabilities would be required for many security-related activities, including internal and external auditing.

Summary of Surveillance:

1. A surveillance mechanism should enable installation management to detect designated system events and designated user activities and to take appropriate steps, either in real-time or post facto, as a consequence of their occurrence. This capability is essential to achieving personal accountability of people for their activities on the system.
2. The surveillance mechanism should enable installation management to designate which events and activities (and characteristics, such as participant people and resources, or time of day, or values of data fields) should trigger a surveillance reaction. Such designations should be simple for management to establish and modify.
3. The surveillance mechanism should offer a menu of actions that may be taken when designated events occur. The selectable actions should include at least journalling of the event, termination of the indicated process, and a real-time alert such as a console message or a bell.
4. The surveillance mechanism should enable installation management to designate which available information is to be journalled for given events. Options should include at least personal identifier, device identifiers, software and data names, an indicator of success or failure of the event, and date and time.
5. The surveillance mechanism design should take into account and where possible, alleviate the problems of archiving voluminous journal data for prolonged periods, even years.

6. The journal should have all necessary protection from all but authorized access. It must be protected from all destructive conditions.
7. The surveillance mechanism may well be multi-purpose, since its capabilities and outputs are also useful for general facility management, including accounting, recovery, load-balancing, tuning, education, and auditing functions. However, a multi-purpose design must not degrade the performance or usability of the mechanism as a security function.
8. The surveillance mechanism should enable installation management to dynamically establish real-time monitoring (display and/or journalling) of the interactive flow of information between a designated terminal or a designated user and the system or subsystem.

System Integrity: System integrity is the condition of proper, predictable, and expected functioning of the total data processing operation, including installed hardware and software and the physical security measures and operating procedures in force at the installation. The system which has integrity is free of significant surprises. System integrity is a fundamental and pervasive attribute of the operation; it certainly cannot be achieved at any installation if individual hardware and software products do not offer high integrity for normal and abnormal operating conditions, including malfunctions, crashes, maintenance and servicing situations, and so on.

The following sections discuss hardware and software integrity at length. Physical security and operating procedures are not discussed in this paper. See the Bibliography for appropriate references.

Hardware Integrity: The following is a brief list of hardware integrity factors which should be included in any list of things for consideration by system implementors:

1. Positive unique device identification is an integrity requirement. It is discussed fully in the Identification section. Devices attached through the switched telephone network must offer the "hard-wired" self-identification capability or the equivalent. Other devices may be adequately identified through cabling addresses, "station ID" addressing protocols, and so on.
2. Error detection and correction capabilities must be such that no single element failure can result in an undetected error.
3. Appropriate devices should offer a facility to clear the residual contents of buffers, electronic storage areas, and all or portions of portable media.
4. Remotely-located devices might require a key-operated power on/off switch. Certain devices (particularly intelligent terminals and communicating typewriter devices) should have major functions (such as transmit, receive, typewriter-only) controlled independently by key-operated switches or a single key-operated multi-function switch.
5. Interactive terminals should have a print/display inhibit capability. This should be automatic where possible. It must be controllable from the system.
6. Appropriate devices should offer positive verification of mechanical operations, as is the case with seek verification in disk devices.
7. Microcode modification in any device should be controllable through a key-operated switch.
8. Processing units must offer store and fetch protection and at least two privilege states.
9. Power failure protection should be such that installation management can ensure that no failure will result in irretrievable data loss.
10. A line-break sensing capability must be offered with all communications equipment such that all conditions of potential disconnect/reconnect (such as transient noise or other switched-network disturbances) are made known to the system, which can then invoke device-ID reverification procedures.
11. External storage device design must be such that there is no possibility of an "undetected mount" situation.

12. External storage devices should offer, as an extra-cost feature, key-operated locks that prevent unauthorized removal of portable media.

Software Integrity. This section is concerned with operating system integrity, which may be described as the ability of an operating system to resist any compromise of specified or implicit security controls that may occur through misuse or manipulation of defined or undefined software interfaces.

Software integrity has received considerable attention in the last few years. The number of environments in which it is considered important to show that independent (and occasionally assumed to be mutually hostile) processes are well-isolated, has grown suddenly in the last decade to include not just a handful of national defense installations, but service bureaus, educational institutions, law-enforcement agencies, banks, research organizations, and many commercial enterprises.

With this increased attention, numerous research efforts are under way exploring such areas as formal proofs of program correctness; operating system "kernel" structures that, partially because of their limited size, can be proven to isolate and control all processes and resources; automated integrity-flaw pattern recognition techniques for operating system analysis, and new processor architectures employing a variety of isolation and modularization approaches such as a large number of privilege states.

Except for certain transaction-driven systems in which terminal users can be effectively denied direct access to system resources, virtually all general-purpose systems are to some degree dependent upon software integrity for the security of the data in the systems.

Historically, operating systems have been designed with the assumption that user programs will be written without intent to overreach implied limits of isolation. No program, for example, would supply an unexpected parameter value, or attempt to gain supervisor state. Also historically, a great deal of money has been spent by vendors and their customers in modifying code to be in line with more realistic design assumptions.

With more recent systems, fewer such assumptions about the benevolent behavior of programs have been made.

It is difficult to overemphasize the importance to data security of some of the more recent developments in the management of programming staffs. The adoption of what is variously known as "structured programming" "top-down programming" or the "chief programmer" method promise not only enhanced productivity and fewer errors but also tend to force programmers into collusion with others if they are to get dishonestly conceived and written code into operation.

Software integrity does more than enhance data security. One important and very desirable effect is a significant reduction in system incidents. Since a high-integrity operating system is one

in which all significant interfaces must be formalized and protected, this reliability phenomenon is not too surprising. The operating system well-insulated against damaging and destructive effects of erroneous code within itself and in its application programs, will be more stable.

Cryptography: Cryptography is not necessarily an essential ingredient in any complement of security measures. Most systems do not need it at the present time. However, it may be much less costly if included into the design of a new system than if it is added to an existing one. It may be reasonably anticipated that the need for cryptography will evolve and so a general understanding of the considerations associated with its use is desirable.

Cryptography (crypto) is the transformation of data from a clear form into a secret form (encryption) and the reverse (decryption) using a process intended to be fully known only to the cooperating proper communicators of the data. It is used when the medium containing or conveying the data (microwave transmissions, for example) cannot itself be protected adequately. The intent of encryption is to make intercepted data useless to the interceptor by making it too difficult or too expensive for him to derive the original clear data in time to use it for his purposes.

The list of threats against which crypto may afford the least expensive practical protection is not a long one. It includes interception of radio transmissions, passive wiretapping (recording or "listening in on" transmissions), active wiretapping (deletion, modification, or destruction of messages, or insertion of false messages, by the wiretapper), accidental substitution or deliberate masquerade of one device as another, and theft of or undetected interference with data that is resident on removal media or even, in some applications, in main storage.

Protection against threats to electronic communications is called COMSEC (Communications Security); protection against threats to data resident in storage media is called FILESEC (File Security).

The National Bureau of Standards has selected a candidate cryptographic algorithm as a proposed Federal Standard. A detailed description of it is beyond the scope of this paper. The following paragraphs provide a brief discussion of considerations in the application of cryptography.

Cryptography for COMSEC: Session crypto is the encryption/decryption of data transmitted between two end-user mechanisms communicating during a teleprocessing session. If there are intermediary devices along the communication path, session crypto is transparent to them. The key used in a given session is persistent at most for the duration of the session (it may be changed in mid-session if the design of the session crypto process allows for this). It is generated randomly and is assigned to the specific session at the initiation of that session. If the key is transmitted over the network, it must be safely transmitted (itself encrypted under some other key known to each of the communicating devices) to one end-user device from the other (or to both from some third device), and dynamically or, under some conditions, manually set in the participating end-user devices. Data encrypted at the originating device for a given transmission is not decrypted until it arrives at the destination device; the fact that it is encrypted need not be known to intermediary devices. Session crypto implies integration of the crypto mechanism into participating devices, at least to the extent that the system itself can control the setting of keys and the switching of crypto devices on and off. It does not imply any crypto capability in devices other than at the ends of the session communication path.

Link crypto is the encryption/decryption of data only across the medium connecting two directly communicating devices. This is the classic cryptographic structure typically used in electronic communications. It is logically independent of the system and does not necessarily imply that the crypto mechanism is integrated into the communicating devices. It can be thought of as implemented by a pair of crypto mechanisms bracketing the line between two communicating devices; each crypto mechanism in this case would be situated between the communicating device and its modem. Link crypto key need not be system settable, and the system need not be able to switch the crypto mechanisms on and off (these operations may be accomplished manually). The link crypto mechanisms, however, must not encrypt line-control information unless they are physically sited outboard of the line-control logic at each end of the link; thus, if the crypto devices are not outboard (stand-alone), there must be sufficient intelligence in the link crypto mechanism to distinguish line-control data (not to be encrypted) from message content (to be encrypted), and implies that link crypto devices for different line disciplines must themselves be different.

Personal-key crypto is the encryption/decryption of data using a key associated with (and manually set into the terminal's crypto mechanism by) an individual user. The personal key need not be transmitted within the system in any form under any conditions. The personal key capability can be used in two fundamentally different applications:

1. The first application is one in which a person's key is known to and used by the system for transmissions involving

that person. In this application, once the person's identity is established (in the clear), the system loads his personal key at its end, the user loads his personal key at his end, and communications henceforth, during that session are encrypted under that key. In this mode, the effect is similar to that of session encryption; if there are intermediary devices, they need not be aware that the data they are forwarding is encrypted.

Data is encrypted/decrypted only at the terminal and at the host for that session. If the session is between two terminals, with the host acting as an intermediary message-switching or processing device, then either both people must employ the same key or the system must employ two personal keys and perform an intermediary decipher/encipher operation as it receives/transmits data between the two terminals. In any event, in this application encryption and decryption occur at both ends of the session's path. If the system has been so designed, installation management might require that all sessions of a given user be conducted using his personal key. This forces him to present his key in order to do his assigned work. If he does not load his key, his output will be unintelligible and his input will be deciphered by the host into meaningless characters. The installation might elect to leave the encryption decision up to the individual on a per-session basis.

2. The second major application of personal-key crypto is the situation where only the terminal end of the session path encrypts and decrypts data. In this application, the system need not contain the individual's personal key or even be aware that encryption is taking place. The data entered into, manipulated within, and withdrawn from the system by the user remains encrypted while within the system. Individuals sharing access to the data must share the key.

The data can be processed only in a limited way (using text-editing-like functions such as block insertion, replacement, moving, and deletion) because encrypted values usually cannot be handled arithmetically and logically like the same values in the clear; an encrypted "2" and an encrypted "3" do not add to an encrypted "5", for example. This is a very powerful method of maintaining the security of data within the system and despite its constraints it has been found useful and is potentially an important application.

Cryptography for FILESEC: FILESEC is the protection of data that is not in transmission but is resident in a storage device. The FILESEC crypto function encrypts data which needs this protection while it is on-line, in the library, in shipment from one place to another, or even in main storage (but not in active processing).

The result of the FILESEC operation is that the data and the key used to encrypt that data are encrypted and stored in some medium. The original clear data may be recovered from the FILESEC medium on the original system or on another system equipped with the FILESEC function.

A convenient and secure way to preserve the identity of the key used to ENCRYPT the data on removable media is to assign identification characters to the individual keys. The key identification can then be recorded directly and in the clear on the medium label. The key-ID/key correlation tables can be preserved in a secure manner at all locations authorized access to the protected, stored data, with each table encrypted under a locally-assigned key. Each table should contain the keys to only those files to be used at that location or facility.

Handling Cryptographic Keys: The most sensitive element of the encryption process is the particular key used to encrypt a given object. In fact, the usual measure of strength of the cryptographic process is the difficulty of deriving this key. For the encryption process to provide security, the keys must be unavailable to any person or process other than those charged with generating, setting, and invoking (and keeping back-up copies) of those keys. Key handling must be reduced to a viable physical security problem. It must be possible to show that the keys are not exposed to tampering or disclosure while they are within the system; that they are exposed only insofar as their physical records, kept outside the system as they must be by management, are imperfectly protected.

This implies that keys must not exist within the system in clear form except when they are actually placed in one of the registers within the crypto device. These registers contain bit patterns currently in use as keys for ongoing encryption and decryption operations. The crypto device should be designed such that physical access to registers within it is destructive to its contents (so that microprobing, for example, cannot succeed in disclosing any key).

Where keys must exist in some form within the system but outside the crypto device, as in transmission of session keys and in tables associating specific keys with keynames and with persons, devices, links, ongoing sessions, and files against which those keynames are mapped, the keys themselves must be encrypted.

The software processes that initiate key transmissions, maintain the tables of keys in storage, and control the functioning of the crypto devices must be shown to be perfectly secure against any improper use that negates the crypto (turns it off, or fixes one key permanently in the crypto device, or modifies the key tables) or yields any key in the clear. By extension, the basic instructions, commands, and orders at the machine instruction interface and below that control the functions of the crypto device must be shown to be proof against any uses (including unexpected and apparently illogical coding sequences) that modify the proper behaviour of the crypto device or that yield any key in the clear in any location or form accessible to any process other than the crypto device itself. The functions of the crypto device that must be protected include on/off switching, mode setting, encrypt/decrypt data commands, encrypt/decrypt key commands, and load key register commands.

Any system process used for random key generation (for session and FILESEC keys, for example) must be shown to be proof against tampering or modeling that result in disclosure of or accurate prediction of its outputs.

Any device provided or procedure recommended for use by installation management in physically setting keys within the system (in crypto devices directly or in the system's key tables)

must be shown to be proof against tampering and against any methods of interception that could yield the keys in the clear. Such a procedure might, for example, recommend offline generation and encryption of the keys and their insertion into the system in already-encrypted form, of their insertion in the clear during some period when installation management can dedicate the system (at least the host) to this operation alone.

The Lost Key Problem: When for any reason the key required to decrypt data is lost or unknown, the data itself cannot be decrypted and is lost permanently unless another copy exists. It is just as difficult for the properly authorized possessor to decrypt his data when the key is unknown as it is for the hostile cryptanalyst who never had the key in the first place.

Users must recognize that there is no recovery from the unknown key situation, and must recognize the various ways that keys may become lost or otherwise unknown. They must establish measures and procedures that can be used to minimize the effects of this situation (back-up data), or to reduce or eliminate the possibility of its occurrence (back-up copies of keys).

Crypto keys may become lost or unknown due to hardware malfunction, software error, or human failing in the physical key-handling procedures. The loss of a key is of concern in some COMSEC and all FILESEC applications; to put it another way, it is of concern in every application where the opportunity to recover from key loss or modification by simply resetting with new keys and repeating the operation does not exist.

In any COMSEC or FILESEC crypto application where hardware malfunction results in undetected modification of the key in storage or in the crypto device, or in failure to load the expected key, encryption or decryption of data will proceed using an unknown key. The possibility of recovery depends on the particular application.

In session-crypto applications, when hardware malfunction results in duplicate erroneous modification of the pair of session keys, the effect is not noticeable and does not diminish security; the situation is simply that the generated session key is not the actual key in use. If the malfunction results in failure to load new session keys at the proper time (thus perpetuating one key through a series of sessions that should be using different random keys) the immediate effect is not noticeable but security is definitely lessened. This failure, whether induced or accidental, is difficult to detect and can be very serious. If the malfunction results in modification of or failure to load one of the pair of session keys, then for that session the keys in use at each end-user device are different and the effects in most cases should be immediately noticeable, either by a person who sees garbled message data at his terminal or by a processor that encounters unrecoverable character errors in its input stream. In this case, abnormal session termination should occur, the original data should not be destroyed, and a new session should be initiated with the same or different hardware and new keys. However, if the session is a one-way data transfer only, with no processing at the receiving end that is likely to detect irregular or illegal bit patterns, and the session goes to normal completion, and the application is designed to destroy the original data upon normal session completion, that data may be irretrievably lost. Such session applications, when the original

data to be destroyed is in fact the only existing copy of the data, should include checking protocols that verify positively that the transmission was successfully completed with proper keys in use before the original data is deleted. Should a failure be detected, the session should be entirely redone.

It should be pointed out that such verification is not simple. It requires superencryption (double encryption) by the receiving device under the receiving device's own active key, and then transmission to the originating device for double decryption under that device's active key. Standard verification patterns and protocols may be employed, but these introduce some security weaknesses if their existence is known to the hostile cryptanalyst.

In link-crypto applications, hardware malfunction cannot result in duplicate erroneous modification of the pair of link keys (unless induced by human intervention, which is a problem addressed by the physical security measures protecting the linked devices) because the keys are set separately and do not have a common system source. Hardware malfunction could result in failure to employ crypto at one end of the link, or in modification of one of the pair of link-crypto keys. Both these errors should be detected at once because of the garbled data received at each end of the link; however, in the data-transfer application described above, under session-crypto, where the data is handled as image patterns and there is no checking for illegal patterns, the data could be irretrievably lost. Further, because the session is not terminated, there could be a serious security exposure on top of this if the data were transmitted in the clear, where malfunction results in failure to employ crypto at either end of the link, the situation is very serious from the security point of view but data will not be lost. It should be noted that where line-control data is encrypted/decrypted, discovery of malfunctions (except those resulting in no crypto at either end) should be immediate in every case. Where, as described above, link-crypto failure can result in apparently successful transmission of data but in fact the data may be lost, it should be kept in mind that the situation differs slightly from the session application in that where link crypt is in use any verification process may have to occur further along in the network than within the device to which the originator is immediately linked. The original and only copy of the data may have to be retained, not merely until the transmission across the first link is completed, but until the data reaches its ultimate destination; and this may take some time depending on the nature of the network and of the software application in use.

In personal-key applications where both the terminal and the host employ crypto, the exposures resulting from hardware malfunction and the concomitant verification requirements are as described above under session and link protection.

In personal-key applications where only the terminal

encrypts/decrypts data, the data may be lost in some situations. If a malfunction results in failure to employ crypto, input data will be in the clear. This is a serious security exposure but will not result in loss of the data (it will be discovered later to be in the clear in the system). If malfunction results in use of the wrong key, there may be no recovery unless the originator has a copy of the data he entered (which should be a standard procedure for this application). If the magnetic striped card containing the personal key has been damaged, resulting in use of the wrong key, the data in the system (some encrypted under the correct key and some under the wrong key) should be recoverable if the original correct key is known (which should be standard procedure; management should have a record) and the current incorrect key is still on the stripe.

In FILESEC applications, hardware malfunction resulting in failure to encrypt data is a serious security exposure but does not cause data loss. Malfunction resulting in modification of the correct key can result in data loss, and verification protocols should be put in place when the FILESEC-protected data is the only existing copy. Also, in FILESEC applications, when the only copy of the random file key is stored on the medium with the data, damage to the volume (broken tape, etc.) may cause loss of the key, and this means the data cannot be decrypted. Management should ensure that, where the application warrants, duplicate back-up copies of the FILESEC-protected data are available. Management should also ensure that the file master key is protected such that its loss is extremely unlikely or impossible. Copies of that key should be maintained in several physically secure and geographically separated locations.

In both COMSEC and FILESEC, software errors and human failings (in designing and following procedures) can result in irretrievable data losses, generally in scenarios similar to those described above for hardware malfunctions.

Performance, Storage Requirements, and Human Factors: It is widely assumed that security features, functions, and procedures are invariably costly to an installation in terms of performance degradation, storage requirements, and human resentment and enforced awkwardness. Close inspection of experience, however, shows that while in a sense, some of this is true; and certainly it can be made to be true; it is largely fallacious. Installations, that have taken the trouble and spent the money to achieve high levels of security have usually found significant benefits that more than justify the security effort.

Among the positive side effects which installations have unexpectedly encountered, are improved total performance of the system (which shows higher reliability and availability because of its increased predictability) and of the entire installation (because overall operation and threats to the smooth continuity of that operation are better understood and can be better controlled through security functions and through improved policies and practices). Human acceptance problems have been seen to disappear rapidly, once users and management recover from the shock of change and fully understand the improved protection and service that security measures give each of them.

Nevertheless, product designers have the responsibility of minimizing impacts in each of these areas. Generally, good design practices should yield good performance, storage utilization, and human factors. The following guidelines merely highlight significant objectives:

1. Performance degradation, if any, should be directly proportional to the extent to which management employs available security features and functions.
2. There should be no measurable performance degradation associated with use of identification/verification mechanisms.
3. Degradation should be expected with use of authorization mechanisms, but only as a function of the degree to which the full capability of the mechanism is employed for a given operation. An objective should be not more than 5% degradation (job running, response time, and system-wide measurements) attributable to any use of an authorization mechanism, however complex.
4. Degradation due to real-time surveillance activity (including journalling but not post-processing or data reduction) should be a function of the degree of use of the mechanism.
5. Degradation attributable to integrity mechanisms should be imperceptible.
6. To the extent possible, degradation should be experienced

only by processes invoking the security mechanisms.

7. To the extent possible, security-related software design should not only minimize performance impact but must take pains to make efficient use of storage, especially real main storage.
8. Security functions should be designed with great care, keeping management's objectives of strong protection, good cost/performance, and high usability in mind, but not neglecting the individual user's day-to-day working requirements, principally transparency of the added protection and ease and naturalness of any actions required of him. Security features and functions should be sufficiently flexible that managements in widely varying environments can adapt them to local security needs while in no case being forced to impose an unrealistically burdensome working environment upon the individual users.

Optionality: Optionality of the security mechanisms is an important consideration where performance and usability are concerns.

Optionality, or the ability to include in the ongoing operation, to exclude, and to define parameters for certain security functions which may be individually selected and used, must exist both at the installation management and at the individual user levels. Management must be able to specify which functions shall be included in all operations; for example, which personal identification and verification procedures must be followed, which events will always be journalled. Management should also be able to permit individual users to make certain security specifications regarding their own operations, such as electing to have individual sessions encrypted, or to have LOGON personal ID verification or additional journalling for specific events take place when management does not generally so require.

1. Security features and functions should be optional so that users who do not need them suffer the least possible cost, performance, or storage utilization penalty.
2. Security functions should be implemented so that users may define for their own resources and operations certain management-selected kinds of authorization, surveillance, and other security-related attributes.
3. Security functions should be designed so that installation management (or users themselves, where management so specifies) can establish default, or "automatic", authorization, surveillance, or other security-related attributes for resources and operations under their control.
4. Optionality must in no case enable users to reduce security by overriding management-specified procedures. In general, optionality should result in the ability of individual users only to enhance the security of operations in which they are involved.

Testability: Testing of security mechanisms can be difficult. It is required not only that they do correctly all that they are supposed to do, but also that they do and allow nothing that they are not supposed to.

Since testing a negative proposition is difficult and proving it impossible, the specifications and design of the mechanisms must be clear, complete, and, if possible, all in one place, so that the mechanisms are made easier to review and test rigorously and thoroughly throughout the development process. If this is not the case, the probability of design oversights and flaws will be high.

The design and specification of any security mechanism must be such that conducting adequate reviews and constructing adequate test of the mechanism is made as simple as possible and can be carried on throughout the development process.

Distributed Intelligence: The statements in this paper are worded as though a system configuration include only one control program. Obviously, such is not uniformly the case. Increasingly, configurations include more than one control program in the forms of hardware subsystems, and both together.

It is not our intent to recommend or imply that identification, authorization, surveillance, or integrity mechanisms must exist physically in one place in a given system.

The intent of distributed processing is to make overall system operation more efficient in some way. No security mechanism should lessen this efficiency by requiring that some function (for example, authorization), that could or should be placed partially in an outboard processor or internal software subsystem controlling some subset of system resources, be kept inboard or in the master control program.

What is important is that, however the security mechanisms are structured or distributed throughout the entire system, their effect in enabling management to protect assets be as strong as though they were centralized, or stronger. Thus, if a number of different processes throughout the system keep activity journals, those journals taken together should yield an accurate, usable record of the activities that management wants journalled, and should enable management to reconstruct the entire flow of events that was initiated by a given user regardless of how that user was connected to the system.

Where subsystems strive to be self-contained and self-supervisory, as do certain industry subsystems, appropriate security mechanisms must be placed with each. Their design must be such that management can exercise such control over user activities, and derive such activity records, and maintain such personal accountability of users for their actions, as it deems necessary.

Often intelligence is distributed to permit continued operations when a portion of the system for any reason is not functioning. For example, a system may normally have the host down on weekends, or may lose communications with the host because of some disruption of the lines or the host operation. In all cases, security capabilities under restricted operational conditions must be commensurate with the limited functions remaining.

1. However the security mechanisms are distributed in complex systems throughout the master control program, software subsystems, and hardware subsystems, their effect must be such that installation management can exercise such control over user activity, derive such activity records, and maintain such levels of personal accountability of users for their actions, as it deems necessary.

2. In all cases, security capabilities under restricted operational conditions must be commensurate with the limited function remaining.

Auditing: It is probably fair to say that, in the course of the switch-over in the past three decades from manual systems to automated electronic systems, many well-established and well-understood auditing tools and practices have been neglected. Manual systems were developed over a very long time, were carefully studied by the auditing community, and many "classic" auditing safeguards were developed for and widely used in those systems. In the rush to automation, however, these safeguards were neglected in favor of increases in "useful function"; costs of application development have been high, and relatively little was spent on adapting the manual auditing practices and techniques to the EDP environment.

The management and auditing communities have recognized over the past few years that enterprises are dangerously exposed to losses because EDP systems are insufficiently auditable. Today, the situation is seen as alarming, and a great deal of resource is being applied to try to rectify it.

The present lack of opportunity for independent, detailed examination of the computerized system is a principle problem of auditing today. Most audits must be conducted around the computer, because they cannot go through it. Insufficient information is captured and surfaced. The controls to interpose testing do not exist. Some examinations are achieved through informal modes of operation tolerated by the existing controls, but these modes are not recognized formally and could be eliminated in a tightening of controls. Restoring the level of auditability that was available with manual systems, and supporting and even augmenting it by formal EDP-oriented audit functions, are the principle goals of EDP auditors today.

Elements and Methods of Audit: Auditors examine productive processes and control processes and draw inferences about the results of each. They also examine results and draw inferences about the processes that produced them. In addition, they examine control data retained by the computing system for all processes. Examinations of these areas are uneven and variable over time. They stress what is new, sensitive, representative, suspect, or otherwise worthy of special attention.

Auditors' examination techniques may be either static or dynamic. A static examination inspects a "snapshot" of the system; it determines the character of processes or results at some point in time. A dynamic examination inspects processes in operation, and looks at results as they are formed. Any examination may inspect either real activities or activities performed solely to exercise the examination procedure.

Static Examination: Static examination of productive processes requires that the auditor create flow diagrams of programs, test plans for programs under development, and comparisons of successive versions of programs to verify that changes are authorized. The auditor needs automated tools for these activities. Such tools include program logic analyzers that describe the program's control flow and functions, mapping mechanisms that show how accurately different specification materials (objectives, functional specifications, logic diagrams, code, etc.) relate to each other, program test case generators, program code comparison routines, and so on.

Static examination of the results (data outputs) of productive processes requires that the auditor inspect all or samples of the data against explicit criteria, and manipulate, summarize, and generate reports from the data. General-purpose data-processing functions are usually sufficient for such examination.

Static examination of control processes is not feasible.

Static examination of the results (journals or logs of activity) of control processes does not differ significantly from static examination of the results of productive processes.

Static examination of control data (data management format indicators, authorization tables, etc.) requires that the auditor have ready access to this information. He needs authority within the system framework to display all such information he needs, and should be able to do so simply, with well-formatted outputs.

Dynamic Examination: A dynamic examination looks at a live system while it is processing real data. The examination is not continuous. It is an exception to be accommodated by the system. It is not an integrated function. It involves diversion of control from the real processing to the audit activity; the real processing is suspended but should not be otherwise affected (except that it might be terminated if something untoward is discovered).

The dynamic examination is typically triggered by some pre-specified event, and control is diverted to the auditor's routine. The number of suitable trigger-events is large. They are selected by the auditor. The kinds of processes (responses) initiated by the triggers are many. They are established by the auditor.

The trigger/response relation is called the link. Links may be fixed, variable, or conditional. The fixed link is a simple, permanent relation of trigger and response. It cannot be changed. It may be built-in or "hard-wired". For all executions over time the response is fixed. The variable link is also simple but it can be changed. It is not built-in. For all executions the response is the same until the auditor, externally, changes the response by defining a new one for that trigger. The conditional link is not simple. It is a set of responses, any of which may be selected in a given instance on the basis of trigger-event characteristics and the current state of the system. The set of responses, and the definition of conditions determining their selection (decision rules), are provided by the auditor.

To conduct dynamic examinations, auditors must employ tools that are fixed or variable or conditional links. Of these, the fixed link is the least useful. It is local and inflexible and will only detect a limited set of tampering cases. The variable link, because it is simple, offers better performance than the conditional link and is preferable where a simple link is sufficient. Because the variable link is limited (one trigger, one predetermined response action), however, the conditional link is generally preferable. It is most flexible and can handle a large number of conditions present at the trigger-event requiring a correspondingly large variety of responses; which may be selected either directly according to sensed input conditions or indirectly according to further computation within the response mechanism.

Among the dynamic examination auditing tools required, in addition to several data-retrieval and data-manipulation tools used in static examination, are those which support tag-trace operations, parallel operation, test monitoring, and input control.

Tag-trace is an auditing operation in which a tag, or special data field not accessible by the general user, indicates to the

auditing process that the tagged record is to receive special processing. The recognition of the tag, the special processing, and the journaling of the tagged item's activity together comprise tracing.

Parallel operation is the interleaved execution, upon test data of real "production" code and of test code (designed to accomplish the same processing and outputs). Interleaving may be at the machine instruction level or at some higher level (subroutines, etc.) if more convenient. The intent is to determine the integrity of the production software, the accuracy of its operation, and any evidence of tampering.

Test monitor functions enable the auditor to generate input streams for processes, to record the execution of control paths (revealing unexpected code and untested paths), and to assess the validity of outputs resulting from known controlled inputs.

Input control operations seek to ensure that the system is properly accepting correct inputs, properly rejecting incorrect inputs, and properly accounting for and reprocessing the rejected inputs when they have been corrected.

It should be noted that many of the functions described under Surveillance are useful for auditing operations.

1. System, subsystem, and application designers must attempt to understand the needs of the auditors and include functions within their designs that will improve the auditability of installed systems.
2. The auditor is in a special position with regard to access to system resources and control functions. He is a potential security threat, because his work requires broad access capabilities. Both the security functions and the auditing functions must be designed to ensure that the auditor's operations are properly controlled and that he can be held properly accountable for his activities.

Documentation: Data security features are not trivial to design and implement such that they are properly integrated into systems, nor are they always simple to understand and employ correctly.

Proper planning, design, and implementation of security features cannot be accomplished unless the requirements and proposed features are addressed explicitly and in detail in formal documentation at every stage of development. They require separate treatment in such documentation. Discussions of security material should not be scattered throughout the documentation; if it is, probably the set of security material discussed will not be coherent or consistent.

8.0 BIBLIOGRAPHY

Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896, Dec. 31, 1974.

Privacy Act Implementation Guidelines and Responsibilities, Office of Management and Budget, Circular No. A-108, Federal Register, Vol. 40, No. 132, p. 28947, July 9, 1975.

Supplementary Guidance on Implementing the Privacy Act, Office of Management and Budget, Federal Register, Vol. 40, No. 234, p. 56741, Dec. 4, 1975.

British Computer Society Code of Good Practice, National Computing Centre Ltd., London, England, April 1973.

H. Feistel, "Cryptography and Computer Privacy," Scientific American, Vol. 228, No. 5, (May 1973).

J. Martin, Security, Accuracy, and Privacy in Computer Systems, Prentice-Hall, Englewood Cliffs, New Jersey, 1973.

H.J. Orceyre, "Data Security," Journal of Chemical Information and Computer Sciences, Vol. 15, No. 1, (Feb. 1975).

D.B. Parker, Computer Abuse, Stamford Research Institute, Menlo Park, California, Nov. 1973.

Privacy in a Free Society, Roscoe Pound - American Trial Lawyers Foundation, Cambridge, Massachusetts, June 1974.

F. Pomeranz, Securing the Computer, Coopers and Lybrand, New York, 1973.

Publications of the U.S. Department of Commerce, National Bureau of Standards:

Executive Guide to Computer Security

NBS Special Publication 404: Approaches to Privacy and Security in Computer Systems, September, 1974.

NBS Technical Note 780: Controlled Accessibility Bibliography, June, 1973

NBS Technical Note 809: Government Looks at Privacy and Security in Computer Systems, February, 1974

NBS Technical Note 827: Controlled Accessibility Workshop Report, May, 1974

NBS Technical Note 876: Exploring Privacy and Data Security Costs - A Summary of a Workshop, August, 1975

FIPS PUB 31: Guidelines of Automatic Data Processing Physical Security and Risk Management, June, 1974

FIPS PUB 41: Computer Security Guidelines for Implementing The Privacy Act of 1974, May, 1975

FIPS PUB 39: Glossary of Terminology for Computer Systems Security, to be published January 1976. Available as TG-15 Working Papers of 9/75

Encryption Algorithm for Computer data Protection; Federal Information Processing Standard, proposed, Federal Register, Vol. 40. No. 149, p. 32830, August 1, 1975

Working Papers of Federal Information Processing Standards Task Group - 15:

TG-15/24.1: Index of Automated System Design Requirements as Derived from the OMB Privacy Act Implementation Guidelines, August 12, 1975 (to be published as NBSTR).

TG-15/30: Toward a Taxonomy of Computer Security Requirements for Federal Agencies, by Alfred M. Pfaff

Publications available from International Business Machines Corp., White Plains New York:

Data Security and Data Processing, Volumes 1-7, Joint Study by IBM Corp., Massachusetts Institute of Technology, TRW Systems, Inc., and the Management Information Division of the State of Illinois (G320-1370 through G320-1376).

Considerations of Data Security in a Computer Environment (G520-2169)

Considerations of Physical Security in a Computer Environment
(G520-2700)

42 Suggestions for Improving Security in Data Processing
Operations (G520-2797)

The Fire and After the Fire (G520-2741)

Proceedings of the IBM Data Security Symposium, April 1973
(G520-2838)

Proceedings of the IBM Data Security Forum, Sept. 1974
(G520-2965)

"OS/VS2 System Integrity," W.S. McPhee, IBM Systems Journal,
Vol. 14, No. 3, 1975 (G321-0042)

An Executive's Guide to Data Security (G320-5647)

Data Security - Threats and Deficiencies in Computer
Operations (G320-5646)

[From *American Scientist*, March–April 1975]

PRIVACY AND SECURITY IN COMPUTER SYSTEMS

(Rein Turn and W. H. Ware)

Dr. Rein Turn received the Ph.D degree in engineering from UCLA in 1963. In the same year he joined the Information Sciences Department of The Rand Corporation. In addition to information privacy and computer security, his interests include computer applications in complex systems and technological forecasting. He has published more than 30 articles and a book on these topics.

Dr. Willis H. Ware received the Ph.D. in electrical engineering from Princeton in 1951. A pioneer in the computer field, he joined The Rand Corporation in 1952. After serving as Head of the Computer Sciences Department from 1964–1971, he is currently a senior member of the Corporate Research Staff. Dr. Ware was the first Chairman of the American Federation of Information Processing Societies (AFIPS) and Chairman of the HEW Secretary's Advisory Committee on Automated Personal Data Systems. At present he is Chairman of the AFIPS Committee on the Right to Privacy and a member of several government advisory committees. Dr. Ware is the author of a book on computer design and of numerous papers on future developments in computer technology and their societal impact. Address: The Rand Corporation, 1700 Main St., Santa Monica, CA 90406.

Computers and their applications in the 1970s differ dramatically from those visualized in the early 1950s when the computer age had its beginnings. Instead of remaining complex and esoteric computational aids to mathematicians and scientists, modern computers have found their most important function in general information processing—storing and manipulating strings of text. Their users need not be highly trained mathematicians but can be office workers, clerks, students, and, of course, researchers in all fields of science and engineering.

Modern computer systems serve many users simultaneously and permit on-line programming, job execution, and data file manipulation from remotely located terminals. The computer's capacity for time-sharing and multiprogramming gives each user the impression that the entire system is devoted to his own exclusive use. Data files and programs may be shared, and users can interact with their programs as they are being processed. This mode of operation is controlled by the operating system software—a set of program modules that control the flow of users' programs and service requests, allocate system resources, schedule execution, handle errors, and keep users and their programs from interfering with each other. An important function of the operating system is to protect users' programs and data files against each other and, indeed, against themselves.

It is necessary to isolate processes (programs in execution) and to protect their working memory space and permanent data files in order to prevent them from being destroyed or modified by inadvertent pro-

gramming or operating errors or by deliberate actions of malicious users. In addition, access to any computer system must be controlled to assure that proper charges are made for the use of the system resources—that no one receives free services at the expense of someone else. However, there are other reasons for providing protection to the computer and its data files.

In business and industry computers are employed to automate a variety of accounting and record-keeping applications. The information involved, detailing production, marketing, finances, and new product development and research, could be extremely valuable to competitors. Industrial espionage, or gathering “marketing intelligence” as it is sometimes called, has become a large-scale activity in the United States.

Computerization of daily business operations has also provided new opportunities for white-collar crime—embezzlement, falsification of records, and larceny by employees. Numerous case histories show that employees who design the systems, write the programs, and operate the data-processing equipment have many opportunities for such acts. Some abuses that the computer makes especially easy are payments for fictitious purchases or to fictitious employees, manipulation of credit levels, and deposits of nonexistent payments into various accounts. Business firms, too, may use computers to embezzle their customers or stockholders. In the Equity Funding Corporation case the company greatly inflated its financial report and, thus, the attractiveness of its stock, by listing fictitious assets and using its computerized accounting system to mislead the auditors. The loss to stockholders and financiers was many millions of dollars.

In government, business and industry, and educational institutions computerized personal information record-keeping systems are maintained for administrative, investigative, statistical, or research purposes. Information in administrative databank systems is used to make routine decisions about individual data subjects (e.g. to grant or deny benefits, credit, employment, admission to a university), to establish their connections with activities under investigation (e.g. organized crime), or to correlate and aggregate their characteristics or behavior patterns with those of other individuals to obtain statistical summaries, behavior profiles, and correlations. In these systems privacy and other individual rights of the data subjects may be violated by unwarranted collection, use, and dissemination of personal information.

Furthermore, consolidation of record-keeping into computerized systems sets up highly centralized, easily identifiable targets for disruption and sabotage by disgruntled employees or by those disagreeing violently with the policies or activities of the computer system owner or users. The acts themselves may range from firebombing of computer centers to “boobytrapping” of programs to destroy themselves in case the programmer is dismissed. Table 1 summarizes the history of computer abuse. It is likely that there are many other cases that have not been discovered or were not reported.

Although manual record-keeping systems and data files are subject to similar threats, certain characteristics of information storage and processing in computer systems make threats to these systems more serious. First, information is stored in the form of magnetization or

voltage-level patterns that are not directly readable by users. They can be altered without a trace of evidence. Computerized records do not have signatures or seals to verify authenticity or to distinguish copies from originals, and they can be manipulated electronically from terminals remote from the physical storage of the data. Transactions can be performed automatically at high speed without human monitoring or intervention. Finally, processing rules are expressed in programs stored in the same devices and in the same manner as data, and they can thus be changed easily and without trace. Such programs are complex and difficult to validate. On the other hand, a properly designed and implemented computerized information system can control errors and manage access to the records much more effectively than any manual record-keeping system.

TABLE 1.—CASES OF COMPUTER ABUSE REPORTED AND VERIFIED

Year	Financial fraud	Theft of information or property	Unauthorized use	Vandalism	Total
1969.....	3	6	0	3	12
1970.....	7	5	9	8	29
1971.....	22	18	6	6	52
1972.....	12	15	16	12	55
1973.....	21	15	8	9	53

In this paper we will examine the protection of privacy and other individual rights in personal information databank systems, maintenance of information confidentiality in statistical research data bases, and implementation of data security techniques against malicious users and external penetrators.

PRIVACY

Let us turn first to the issue of privacy, which in the context of this discussion refers to the rights of the individual regarding the collection, processing, storage, dissemination, and use of information about his personal attributes and activities. In one proposal, these rights are embodied in a Code of Fair Information Practices, conceived by the Special Advisory Committee on Automated Personal Data Systems to the Secretary of the Department of Health, Education, and Welfare. The code rests on the following basic principles, which are equally applicable to personal information databank systems in the government and in the private sector: (1) There must be no personal data record-keeping systems whose very existence is secret; (2) there must be a way for an individual to find out what information about him is on record and how it is used; (3) there must be a way for an individual to correct or amend a record of identifiable information about him; (4) there must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent; and (5) any organization creating, maintaining, using, or disseminating records of identifiable personal data must guarantee the reliability of the data for their intended use and must take precautions to prevent misuse.

All personal information databank systems would be subject to these requirements and must incorporate a corresponding set of safeguards. Enactment of the code as a federal or state law specifying penalties for noncompliance and establishing an enforcement machinery would be an important step in securing individual rights. Indeed, the United States Congress recently enacted the first such law, the Privacy Act of 1974, signed by the President on 1 January 1975. However, this act applies only to databanks maintained by the federal government. Similar bills are pending in many state legislatures.

Unfair information practices would be subject to criminal and civil sanctions under the code, and victims could recover both punitive and actual damages and obtain injunctive relief. For example, the Privacy Act of 1974 specifies a fine not to exceed \$5,000 for any willful violation of the act by officers or employees of a federal record-keeping organization, or by anyone requesting information from the organization under false pretenses.

The code would require an annual publication, listing the names of record-keeping systems, their nature and purpose, their data sources, the categories of data maintained, the identities of agencies that routinely use the records, and each agency's policies regarding the storage, retrievability, access controls, retention, and disposal of the records. It would regulate the behavior of organizations maintaining personal information record-keeping systems by requiring them to identify an arbitrator to whom complaints could be directed; to take affirmative action to inform employees of safeguards and to specify penalties for any infraction of them; to take precautions against transferring identifiable personal information to other record-keeping systems that may not include adequate safeguards; and to maintain records with an accuracy, completeness, currency, and pertinence consistent with their intended use.

Individual rights would be explicitly guaranteed by the code. When asked to supply personal data, an individual would be informed whether he is legally required to do so or whether he may refuse. Upon his request, he would be informed whether he is a subject in a given data system, and he would have the opportunity to inspect his record, challenge it, and cause corrections or amendments to be made. In the case of a dispute that cannot be resolved, he would have the right to submit a concise rebuttal, and the data items in question would be marked as being disputed. He would also receive assurance that data about himself would be used only for the stated purposes of the system, and the agency would be required to request permission for and to maintain records of any extraordinary uses.

Nearly all proposed legislation and the enacted Privacy Act of 1974 have adopted the code as the basic framework of privacy protection. Based on the use of existing legal and judicial institutions to implement privacy protection, the code is consistent with the traditional approach in the United States to deterring societally or personally undesirable actions against the individual (e.g. the criminal laws and the unfair labor practices laws). It would create a minimum of new bureaucratic functions. Through court decisions and interpretations, it would provide an adaptive solution to the issue of personal privacy as the attitudes of society and the needs for personal information

change. However, like other social policies developed through legislative and judicial processes, the reforms imposed by the code would proceed deliberately—which often seems too slow to advocates of privacy protection.

CONFIDENTIALLY

In contrast to privacy, which refers to the rights of the individual, confidentiality implies that the data themselves and the information they contain must be protected and that their use must be confined to authorized purposes by authorized people.

Certain categories of personal information are given a confidential status by statutes and laws. For example, the personal data gathered in the United States decennial census are required to be kept confidential by federal law. This means that no individually identified census responses may be disseminated to anyone outside the Census Bureau, and even within the bureau only specially authorized employees are permitted access. Attorney-client information exchanges, certain medical and mental health information, and legal proceedings involving children and juveniles are other examples of information categories protected from general access by confidentiality provisions in federal or state statutes.

Most categories of personal information do not enjoy any statutory protection; however, disclosure of such information may be compelled by legal process, such as a subpoena issued by a court, legislative committee, or other official body that has jurisdiction in the locality where the data are kept. Personal information gathered by educational institutions and by research projects in social, political, and behavioral sciences is very susceptible to these procedures.

The lack of statutory confidentiality of personal information gathered for research purposes in a serious concern to researchers whose studies require the gathering of sensitive personal information. While the researcher may have the best of intentions as far as preventing any dissemination of identified information (and may assure his respondents of the confidentiality of their replies), if faced with a subpoena he has the choice of being cited in contempt and suffering the penalties, or else surrendering the data. In either case his research project has been seriously damaged.

The reality of the subpoena threat against research data bases was demonstrated by two incidents in 1969. One involved an Office of Economic Opportunity-sponsored negative income tax experiment in New Jersey, in which first the county prosecutor and then a grand jury subpoenaed the records. During the same period the General Accounting Office and the Senate Finance Committee also sought to obtain them. In the second case, an investigating commission demanded access to the data on an antipoverty research project in Chicago. The project collapsed.

The Code of Fair Information Practices addresses this problem by seeking federal legislation to protect statistical reporting or research data against compulsory disclosure through legal process. Such legislation would include the following features: (1) Protection would be limited to data identifiable; (2) protection would be specific enough to qualify for nondisclosure exemption under the Freedom of Information Act; (3) protection would be available for data in the custody

of all statistical reporting and research systems whether supported by federal funds or not; (4) federal law would be controlling; no state statute could interfere with the protection provided; (5) either the custodian or the individual about whom data are sought by legal process could invoke the protection, but only the individual would be able to waive it.

Whether or not general statutory confidentiality protection is provided for statistical reporting or research data, the code specifies that the data-gathering organization is responsible for informing the individual subject whether he is legally required to supply the data requested or may refuse, and also of any specific consequences for him, which are known to the organization, of providing or not providing data. It must also guarantee that no use of individually identifiable data will be made that is not within the stated purposes of the system as reasonably understood by the individual, unless his informed consent has been explicitly obtained; and that no data about an individual will be made available from the system in response to a compulsory legal process, unless the individual to whom the data pertains has been notified of the demand and has been afforded full access to the data before they are made available in response to the demand.

Until this blanket protection is achieved, there are several procedural and technical means available to reduce the likelihood of damage to research subjects in case the data files are subpoenaed or otherwise obtained by unauthorized persons. One is exposure reduction, which involves limiting the amount and nature of the data collected. At the risk of reducing the utility of his studies, the researcher refrains from obtaining sensitive information or uses survey techniques that introduce uncertainty in the responses. In the "randomized response" approach, sensitive questions are answered only in a statistical manner. For example, a respondent may be given two questions, one sensitive and the other innocuous (Do you take drugs? Do you like opera?). He is instructed to answer one of the questions truthfully but not to indicate which one. Given that statistics regarding the innocuous question are available, the researcher can estimate the profession of respondent affirming or denying the sensitive question.

Reducing the sensitivity of information and, hence, the possibility that it may be subpoenaed can also be accomplished by the randomized response approach, and by "inoculating" identifiable information with errors in an irreversible but controlled fashion, so that the statistics of the data ensemble remain unchanged but individual responses may be incorrect. For example, the "yes-no" answers to a sensitive question may be changed at random. Of course it is essential to publicize widely that the data files have been contaminated in this way.

The anonymity of information in a statistical databank may also be ensured by removing or modifying a number of identifying data items sufficient to preclude the use of remaining data to identify a specific individual, even if the so-called "twenty questions game" is played against the file. For databanks where identification must be preserved for future updating of the information, a link-file system approach may be appropriate. In such a scheme, the identifying data for each individual are separated from the rest of the record and assigned a random code number. The substantive data are assigned a different

code number. A third data file that establishes the correspondence between the first two is kept at a location outside the jurisdiction of the authorities of the locality in which the data are kept, for example, in a foreign country.

Encoding and encryption techniques can be applied to conceal the stored information or to perform data-merging operations involving two databanks without revealing the information. It is essential, of course, to assure that the keys to encoding and encryption operations are adequately safeguarded. Accountability procedures are also necessary to ensure that a specific databank employee or user is responsible at all times for every sensitive data file or set of records. Finally, access control procedures must be enforced to prevent unauthorized access or dissemination of any sensitive data.

COMPUTER SECURITY

Computer security encompasses the measures required to (1) protect a computer-based system, including its physical hardware, personnel, and data against deliberate or accidental damage; (2) protect the system against denial of use by its rightful owners; and (3) protect information or data against divulgence to unauthorized recipients. Threats that must be averted by computer security measures include natural disasters, riots, equipment failures, negligent or maliciously motivated employees and users, and external intruders. The physical security measures against these threats are well in hand, but their application in a computer facility requires careful analysis and engineering. For example, a ceiling sprinkler system is not a proper fire extinguishing system in a room housing a computer, and a tear gas dispensing system that deters a rioting mob also corrodes sensitive electronic components in the computer circuitry.

Different security measures are required to limit access to programs and data in the computer system to legitimate authorized users. These access control measures must be able to counter actions that covertly capitalize on weaknesses in the computer system that may be unknown even to the system's management. It may be very difficult to determine that such actions are in process or have been completed successfully. For example, if a penetrator succeeds in gaining control of the operating system, he could first disable the accounting and auditing programs and then proceed to read or modify any program or data file without being detected.

Unauthorized access may occur accidentally due to programming errors or malfunctioning equipment, or as a result of deliberately planned activity. In the latter case, the ability of an intruder to gain access to protected resources depends on the structure of the computer system and on the opportunities it provides for interaction. For example, a remotely accessible, time-shared system in which users can submit assembly language programs offers more opportunities for penetration than a system where the users are limited to performing a fixed set of transactions and cannot submit their own programs.

Data security techniques are implemented to prevent unauthorized access or, if absolute prevention is impossible or unneeded, to increase the costs of intrusion to a level where the expected "profits" are un-

attractive. The objectives are (1) Isolation of users and their processes from each other and from supervisory programs, to prevent users' processes from interfering with each other or the supervisor and from capturing control of the system; (2) positive identification of all users and authentication of their identity, and attachment of unforgeable identifiers to all users' processes in the system (the time of creation of the process has been suggested as one such identifier); (3) total access control by the supervisory program over all shared-system and user-owned resources (memory space, subroutines, data files, input-output devices, etc.); (4) concealment of information on removable storage media and in communication channels by privacy transformation (encryption) techniques; and (5) integrity control, ensuring that the protective system is correctly implemented and is not weakened by modification of software or hardware.

Defensive design and application of the principle of least privilege are basic to any data security system. Examples of defensive design include the concentration of software-implemented security functions into security kernels—compact software modules whose correct operation can be proved by formal techniques or by testing; and compartmentation of the system to limit the damage an intruder can do if he does succeed in penetrating some part of the protected system. The principle of least privilege specifies that any user's or system's process be granted only those access rights and privileges it needs to perform its functions. Neither defensive design nor the principle of least privilege has been applied in the design of contemporary operating systems.

The simplest way to isolate a set of users is to process their programs one at a time, completely erasing any portion of the memory space that is available to the subsequent user. This approach is still practiced in processing classified government data, but it is unnatural and wasteful in modern resource-sharing systems. In the newest systems, a common isolation technique is to determine for each user the bounds of the assigned memory space (the lowest and the highest address values he may use) and testing each memory reference to be sure that it falls within these bounds. In computers using the virtual memory concept, memory space is further protected by the users' inability to generate addresses that are outside their own assigned memory space.

The operating system and supervisory programs can be isolated from users by providing two or more system states for the processor (a "user state" and one or more "supervisor states") and a set of privileged instructions. These instructions are used by the operating system for allocating resources, establishing access control privileges, and requesting input-output operations, and they can be executed only when the system is in the appropriate supervisory state. As an illustration, assume that a user process needs to read a set of records from a particular data file. It issues a request specifying the file name and the records involved. The operating system will change the system state to "supervisory" and will test whether the process is authorized to have access to the file and the records involved. If authorization is permitted, it will transfer the requested data into the user's memory space and return the system to "user" state.

IDENTIFICATION

In a remotely accessible computer system, it is necessary for the system to identify positively each user and each terminal. In a multi-computer network, participating systems must be identified to each other and to users. The need for precautions is demonstrated by the so-called "piggyback" system penetration threat, in which an illicit minicomputer-equipped terminal is inserted into a communication line to "manage" a user's interactions with the computer system. The user's sign-on procedure is intercepted by the intruder, who generates the correct responses until the user transmits his password, at which point he is informed of a system failure and disconnected. The intruder then signs on himself using the intercepted password.

The most common technique for identifying a user to the system employs his name, man-number, or account number. The authenticity of the identification is verified by a password. Three approaches to authentication of identity are by means of something the user *knows*, something the user *is*, or something the user *has*. Popular in the last category are badges or cards bearing a magnetic stripe, which can be inserted into a terminal for identification. These cards can be designed to resist forgers and, although they can be given to others, their possession can be made mandatory and is easy to check. For example, the cards may be assigned additional functions, such as operating a card-key lock to gain entry to the terminal room, or they may be required for presentation when submitting computational jobs.

The use of personal characteristics such as fingerprints, voice prints, or hand dimensions is attractive but involves the use of complex devices for extracting the physical variables and formulating them for transmission. Moreover, considerable processing time and storage space may be required. At present these techniques are considered too costly for general application, but future advances in hardware technology may permit manufacture of inexpensive special-purpose processors for fingerprint analysis or voice-print generation. Thus these identification/authentication methods may become economically attractive.

ACCESS CONTROL

A major advantage of many modern computer systems is the ability of users to share programs and data among themselves. However, in order to control this function, the owners of the shared resources must be able to specify to the system who is to have access to data and what processing actions they may take. In return, the system must be able to enforce the rules rigidly not only under static, predetermined conditions but also under dynamic conditions, when authorization changes are frequent. In a dynamic situation an authorized user may generate new processes and data files and wish to pass to others selected access rights, to retract previously granted rights, or to specify the rights-passing conditions within the new processes themselves. Clearly, management of access rights is a complicated task that must be implemented in the system's operating software.

Several conceptual models have been developed for the implementation of access control procedures in operating systems. The basic elements are subjects (programs requesting access), protected objects

(data files, other processes), and access modes (the operations that processes may perform on objects, such as "read" or "modify" data, "execute" a program, etc.). The access control matrix specifies the access rights and modes. Figure 1 illustrates a hypothetical example.

Since an access control matrix is likely to be sparse, it will be uneconomical to store in matrix form. Instead, each object can be provided a list of subjects that are to be afforded access to it (that is, the columns of the access control matrix will be associated with the objects), or, alternatively, each subject can have information that will allow it access to those objects it is authorized to obtain (that is, the rows of the access control matrix will be associated with subjects). In the latter case, a process will have a set of "keys" to open "locks" on protected objects or a set of access-granting "tokens" for presentation to the access control mechanism. Each of these approaches has been implemented in an experimental design.

The situation is more complex if access depends on the data that are being requested. For example, a user may be allowed to process salary information only for employees who earn less than \$20,000 who are members of a particular department or project, or who satisfy some other specified criteria. Each access-granting decision may require a computational-logical procedure of considerable complexity. Further, if proprietary programs are to be used, the owner must be assured that the user does not make a copy for himself, and the user must be assured that the proprietary program does not keep a copy of his data. A mutually suspicious situation such as this may occur with a program for preparing income tax returns. A more detailed discussion of this and other complex access control models is contained in the literature.

In computer-terminal and computer-computer communications links and in removable storage devices, data can be protected against wire-tapping and theft by concealment techniques, including the use of cryptographic transformations. While the basic principles of cryptography formulated for the concealment of natural language still apply, there are certain qualitative and quantitative differences in the application of cryptographic techniques to protect information in computers, and in the use of cryptanalytic techniques by an intruder to gain access to information so protected. Computer-stored data are unlike written or telegraphed messages in ways that may both enhance and diminish the protection provided by encryption. For example, most of the stored data are numerical values, codes, names and addresses, or statements in programming languages. These tend to have more uniform character and polygram-frequency distributions than natural languages. In addition, data and expressions in computers tend to have rigid formats and to follow strict syntactic rules. Large amounts of data are stored, and sizable fragments of material known to occur also in the encrypted files can be expected to be available to the cryptanalyst for use in formulating and testing his hypotheses. Given these differences, and the availability of computers for cryptanalytic purposes, standard cryptographic transformations (both polyalphabetic substitutions and simple transpositions) can be solved very quickly with the help of powerful mathematical techniques. On the other hand, the rapidly decreasing cost of digital hardware will make

it economically feasible to construct special-purpose processors for applications of combined substitution and transposition transformations that approximate the "mixing transformations" recommended by Shannon. For example, the IBM "Lucifer" system could be built with only 4 monolithic microcircuit chips (each containing 280 logic gates) to apply a complex sequence of transformations.

INTEGRITY CONTROL

A comprehensive system of security safeguards is effective only if it is correctly designed and implemented and operates correctly thereafter. The major problem in resource-sharing systems is the design of the operating system software. Large operating systems contain hundreds of program modules and hundreds of thousands of instructions. For example, the MULTICS operating system, which was designed and implemented with data security and access control in mind, contains over 2,000 program modules. Some 400 of these implement functions involved in or critical to the system's security; on the average, each module contains 200 lines of program statements. Despite more than nine years of operational use and continuous testing, occasional errors in MULTICS are still found. Not every error in the operating system software is also a security vulnerability, but many are. Indeed, every operating system now in use that has been tested has been found to contain numerous errors.

Software errors are a general concern, and techniques are being developed to produce more reliable software. But the need for security adds a new dimension to the need for correct operation: not only should programs perform correctly all tasks they are designed to do, but they should also *not* be able to perform any other tasks. Anomalous behavior is very difficult to validate and may require formal proofs of program correctness in addition to vulnerability analyses and penetration testing. All current validation approaches have shortcomings: only very small programs can be handled by mathematical-logical program-proving methods, and penetration testing shows only whether or not a particular test team can defeat the security system. To top it off, all approaches are quite expensive. Vulnerability analysis of a modest-sized operating system may require 3-6 months of work by a team of 3-4 analysts. The average cost per design error discovered ranges from \$100-1,000.

Among the techniques for assuring that security mechanisms continue to function properly are auditing and threat monitoring. Auditing involves continuous recording of information about access control requests and corresponding system decisions for analysis after the fact by security personnel or external auditors. Threat monitoring programs assemble information on the operation of the security system in real time to detect unusual activities. In present systems, threat monitoring is at a very primitive level. Essentially, it counts the number of times a user fails to provide the correct password. More sophisticated threat-monitoring instrumentation presupposes the ability to characterize penetration activities in terms of sets of measurable system variables, plus the ability to distinguish penetration attempts from other unusual but legitimate data-processing activities.

PROTECTION COSTS

Protection costs include the initial cost of establishing a protection system and the recurring operational costs. Typical initial cost items are analysis and specification of protection requirements; design and implementation of policies, regulations, and procedures for providing data security and privacy and confidentiality safeguards; acquisition of protection-oriented equipment and facilities and provisions for physical security; generation, validation, and testing of the system software; and conversion of personal information data files to incorporate protection features.

The initial investment in design will greatly influence the quality of protection achieved. In particular, expenditures for software design, implementation, and validation are the key to the system's effectiveness against possible penetration attempts by malicious users. Experience shows that these types of intrusions are more likely than penetrations from outside.

The operational cost of protection includes the usual overhead, such as salaries, equipment rental, and expendable supplies. It may also include processing time for user identification and authentication, application of access control procedures, and recording transaction logs and audit trails; main- and secondary-storage requirements for the protection programs, tables, and data fields, and for transaction logs and audit trails; computer and personnel time for testing and revalidation of hardware and software after modifications, repairs, or restarts; and personnel training and education in protection policies, procedures, and attitudes.

Further, if processing time and storage requirements for the safeguards are substantial, the computer system may be unable to meet its peak workload demand; the organization may be compelled to reduce service or to acquire more or larger processors or more on-line storage. In general, security mechanisms tend to reduce the general availability of a system to its users, and thus they are in conflict with the traditional goals of systems managers and users—economy, increased availability, and easier access.

The frequency and complexity of the access control decisions that must be made are important variables in the cost of protection. If the access rights of each user are tested only at the initial log-in time, or at the time of the initial file-opening request, the processing requirements may be small relative to the normal file-processing operations. However, cost will escalate when access control tests are applied each time a record is retrieved from protected data files. Furthermore, if the access control decisions are data-dependent, the cost of processing time will be even greater, for every data field must be tested to determine its value and then compared with the parameters specified for the access test. In general, it is estimated that access control features tend to increase the overall processing time by 5 to 10 percent, the operating system software size by 10 percent, and the main memory requirement for the operating system by 10 to 20 percent.

Techniques for data security are evolving rapidly but much research and development remains. Implementation in existing systems is

often excessively costly or even infeasible. Moreover, not all computer systems will require the same level of protection. Those containing personal information that is already publicly available need implement only features that protect data from accidental modification and prevent users from interfering with each other. More sensitive information in on-line, shared, or integrated databank systems may require all the known protective features and more. In fact, extremely sensitive information should not be stored in any contemporary resource-sharing computerized databank system.

[From Arizona Business, March 1976]

COMPUTER SECURITY IN CONCENTRATED INFORMATION SYSTEMS

(Leslie D. Ball and Steven D. Wood)

Information is increasingly being recognized as one of the most valuable resources of the firm. The existence and veracity of information must be maintained to support daily operations, allow accountability, and promote effective decision making. As business organizations are faced with processing greater volumes of information than ever before, they tend to consolidate large amounts of information at central data processing installations. The benefit of such policies include minimization of redundant data storage, processing tasks, and costs, and the opportunity to integrate information from various elements of the firm to attack multifaceted decision problems.

As information concentration increases, however, the interest in, opportunity for, and potential severity of information misuse increases commensurately. Because of this, security in the concentrated information processing environment is becoming a serious issue in almost any firm that creates, maintains, or reports information with a computer. The magnitude of the issue is amplified by the fact that many large computer systems maintain data and programs that have a replacement cost equal to, or greater than, most assets on the balance sheet. And, as direct interaction with computer maintained information has increased, the potential for information misuse has tended to outstrip the means of identifying misuse or protecting the information.

Witness the following examples of information destruction and security breaches:

1. A small airplane crashed into a computer center destroying the computer and injuring many personnel. The computer manufacturer rushed in new equipment restoring normal operation in less than three days.

2. Using the computer as a tool, executives of a California insurance company created 56,000 fake insurance policies and sold them to re-insurers. Insurance Commissioners in at least three states are investigating. The estimated loss is \$2 billion to the re-insurers.

3. A programmer stole \$5 million worth of programs he was maintaining for his employer and attempted to sell them to a customer

of his employer. He was convicted of grand theft and lost two appeals based on programs not being property as defined by theft laws. He served five years in prison.

4. A tape librarian, disgruntled because she was fired, replaced all of the magnetic tapes in a vault with new blank tapes during her 30-day notice period. The loss was estimated at \$10 million.

COMPUTER SECURITY AND PRIVACY

Information system professionals label the issue of information misuse in the computer environment as "computer security" and/or "information privacy." Computer security consists of the physical or procedural strategies developed to prevent events similar to those cited above from occurring. It is best defined as the protection of the computer, the data it contains, and the programs that direct its action from accidental or deliberate destruction, modification, or disclosure. These physical and procedural strategies involve hardware and software protection methods. Software protection methods include such things as sophisticated coding procedures employed in data transmission to prevent use of the data should it be stolen via wiretapping techniques or other covert means. Hardware protection methods include the protection of the computer equipment from various Acts of God such as fire, flood, and windstorms.

Information privacy is a separate, but correlate issue from computer security. While there is no constitutional "right of privacy," the common law right of privacy states that an individual should have legal redress for such things as appropriating his name and likeness for advertising purposes without his consent, or intruding into his solitude, has been extended to include information collected about individuals. This definition has been used as a foundation for the establishment of the Privacy Act of 1974, which controls the use of federal information systems; and House Bill 1984, which extends that control to private information systems. Even though comprehensive legislation has not been passed, manager and users of private information systems cannot ignore the fact that privacy laws will require extensive changes in the way in which information systems are created and used. It is necessary, then, to consider privacy along with security measures.

Computer security requirements share similarities within industries but are unique to each firm. As an example, because its lifeblood is financial transactions, a bank is more often dependent on different aspects of the computer than a manufacturing firm and therefore requires a different security plan. However, a small county bank has needs that differ from a large international bank.

Although industry type and firm size are both determinants of security needs, other factors must also be considered. For example, security needs will be different for those organizations employing data base techniques as opposed to those firms employing conventional file processing concepts. In the remainder of this article a number of such differences will be presented, and security methods for handling these problems will be discussed.

Large concentrations of information are tending to be managed by data base management systems (DBMS) and referred to as Data Bases. The data base contains all of the information that has been collected on a group of people, on a manufacturing process, or on a set of financial transactions. It is used to carry on the operation of the business and assist in management decision making. In contrast to traditional information processing methodologies in which applications and files are processed separately, with a data base approach all of the data elements are "linked," and processing applications often employ the same data elements concurrently.

Data base management systems (DBMS) do not represent radically new methods. Rather, they extend hierarchical file concepts to mass storage files, use list techniques as an aid to accessing files through multiple indexes, and incorporate the storage of file description information as an integral part of the data base. Two key characteristics of DBMS are sharing data between computer programs and structuring data so that ad hoc management requests can be satisfied in a timely manner. These structural and manipulative impositions on the data base are designed to promote greater accessibility, minimize data storage redundancy, and increase the frequency and variety of the use of the firm's information.

Because of the integrated nature of the files, an effective security plan in a non-data base environment may not be effective in a data base environment. In the usual setting each user has access only to his own files, but in a large integrated data base his access must be controlled more closely so that he cannot access information that is not in his user domain. To monitor these activities, transaction logs must be maintained and access controls instituted.

Economy

Given that it is never possible to develop a security plan that offers 100 percent protection, it is necessary to include economy as one of the design criteria. Security needs must be balanced with the funds available, as funds are always a scarce resource and must be shared among other computer system demands.

In an integrated data base environment, a large portion of funds available for the operation of the computer system must be allocated to security measures. Destruction of a file in a non-data base environment creates a certain amount of inconvenience to the department that the file belongs to, but in the data base environment destruction might temporarily cut off information sources to *all* departments. While economy is an important criterion, designers must realize that a large portion of their resources must be committed to the protection of all of the data eggs in the one computer basket.

Simplicity

Simplicity refers to operating simplicity. For example, it is important that the user of a remote terminal have quick access to the system when necessary. He must not be required to input his social security number, his mother's birthdate, today's date multiplied by three plus two, and user code, or he will likely not use the system because of such barriers to efficient access. However, many of these

accessing checks can be eliminated if an adequate operating system security plan is instituted in the integrated data base system. In other words, the system itself can do most of the checking without the terminal operator being required to input excessive information that makes the operation of the system difficult. It must be remembered that the computer is designed to provide a service to its user and if that service is difficult to obtain, users will be less likely to fully utilize the system.

Simplicity must also extend to the operation of control procedures within the computer center, the back-up storage facilities, and other operational areas. In the event that the control procedures are not made simple to operate they will be bypassed and security becomes a myth.

Reliability

Finally, reliability is necessary if the security plan is to be acceptable. The computer system will be of little value if the security plan is unreliable. It is important to catch all of the intruders all of the time rather than catching some of the intruders some of the time. Reliability of a security plan in the data base environment is of particular importance. Failure to catch one intruder could have disastrous results for all users; intrusion might prove untraceable, and the effect would be felt for a long time.

IMPLEMENTING DATA BASE SECURITY

Implementation of a successful security program for a base system requires an extensive commitment on the part of management and the entire data processing staff. The security plan cannot be developed by a single person in most large organizations because the task is involved and requires information that is beyond the reference scope of one individual. Therefore, a team approach is necessary. It is now our intention to examine an approach that might be employed to obtain management's support and to implement a successful security plan.

Team Approach

The team should consist of representatives from the internal audit group, the legal staff, the insurance staff, the data processing department, the financial area, and from some of the larger user departments. In addition, a top management person should be involved in the team's work to display management support. This person should be delegated as the official project leader even if another member of the team actually has responsibility for the team's progress. Each team member will have responsibility over various parts of the project; however, major decisions should have inputs from all team members.

The internal audit group has the responsibility of maintaining control of the accounting function in an organization. In many organizations they have elected to exercise that control up to the point that the records enter the computer and then pick up the control process as the records leave the computer; while the records are in the computer, control is lost. In a large integrated data base, control must

exist throughout the entire record handling process. Therefore, the auditor's responsibility will be to ensure that adequate controls exist while the records are in the computer and to ensure that procedures employed are auditable. Included within this overall responsibility is the requirement that the security plan be auditable as well.

In recent years privacy legislation has been passed in many states as well as the federal government and, currently, more than 100 bills are pending in the federal and state legislatures. This has greatly increased the need for legal advice in the development of a security plan, particularly in an organization that handles personal information. A team member from the legal staff is important to interpret the recent and pending legislation that might affect the manner in which records are processed, and the responsibility of the organization in controlling the use of those records.

Many of the threats to a computer system are insurable. The insurance representative should be responsible for determining what hazards can be insured against. In addition, many insurance premiums can be reduced if certain safeguards are instituted. The team member from the insurance department should be conversant in data processing terms and capable of handling these tasks.

It is necessary to have a member of the data processing department on the team to interpret technical problems involving implementation of the plan. It is important however, for all team members to understand that the resulting security plan will change the manner in which the data processing department operates and, therefore, the data processing member has a vested interest in the outcome of the plan. The nature of this interest must be understood by all team members so that the data processing member cannot unduly influence the action of the team.

A representative of the finance office should also be a member of the team. His responsibility will be to assess the total economic impact of various security threats on the organization and to have responsibility for determining the costs of implementing security procedures.

Finally, representatives of some of the largest users in the organization should be members of the team. These members should be familiar with the automated record handling activities of their departments and should be able to clearly interpret the effect of various threats and prevention measures on the operational effectiveness of their departments.

As members of the security team, the user representatives should develop a concern for security problems in their own departments. These concerns should be shared with department administrators. As the departments become more aware of security problems, the costs necessary to implement security procedures should also become more visible. As these costs must be shared by the various departments, it is important that the department be aware of them and that a departmental representative be involved in the cost allocation of security procedures.

Data processing systems analysts will probably be responsible for much of the research and detail of the implementation plan and therefore should also be involved early in the project.

Risk Evaluation

The first task of the team should be a thorough risk analysis. A risk analysis is done to determine the potential exposure of the organization to various security threats, and to determine the costs associated with each threat. The product of these two items yields an exposure rating measured in dollars per year, which can then be rank ordered to determine which possible threats need protection. Suppose for example, that it has been determined that the probability of a fire in the computer room in any given year that would destroy 50 percent of the equipment and records stored in the room is one in five hundred. Also, that to recover from such a catastrophe would cost \$750,000. The exposure rating for this potential event would be the product of these two factors, or \$1,500. Now, also suppose that a control problem that costs \$5.00 to correct occurs on average twice a day. This event costs \$10/day or \$2500/year given a 250-day year. The \$2500 per year figure can then be used as the exposure rating for the this event, and compared against other events.

Clearly, two things have to be determined to develop an exposure rating and those are the probability that the event will occur and the cost to the organization should the event occur. The determination of probability ratings for each event is not as difficult as one would imagine. Insurance companies can estimate the likelihood and impact of natural disasters if they are afforded specific characteristics of the operational environment of the computing facility. For cases involving control problems, historical evidence within the specific organization will provide input to estimates of the frequency and severity of the difficulties. This data can be collected from control clerks and an analysis of job re-runs made by the system. The most difficult probabilities to estimate are those involving fraud. In most instances an educated guess will have to be made based on an estimate of control employed in that functional part of the firm.

Costs, nevertheless, are easier to estimate than probabilities. Quite frequently, however, all associated costs are not included thereby yielding a cost that is less than should be used in calculation of the exposure rating. As an example, consider the case of a fire in the computer center. The most obvious cost is that of acquiring new equipment to replace the damaged equipment. Equally obvious are the costs associated with the reconstructing of any master files that might have been damaged.

To return to normal operations requires a number of other less obvious costs. First, it might be necessary to rent computer time and even temporary quarters to house the computer center and the staff. It may be necessary to pay for orders of business forms and other essential operating supplies. Additional staff will be required to supplement the existing operations personnel in returning to previous processing levels, and if required, to replace incapacitated employees. Finally, it is quite likely that this business interruption will result in delays to other functional areas; it could even result in the loss of some business. All of these items can be estimated to arrive at a proper cost estimate for a fire occurring. Similar consideration should be given to all possible events.

Security Costs

It is essential that the security team be able to determine the actual costs of the protection procedures. These costs will be broken down into initial capital investments and continual operating costs. However, many protection methods can be employed to protect against more than one threat, and the costs must be allocated to each carefully.

When the costs have been determined it should be possible to compare the reduced exposure rating with the cost of instituting the security measure. Security measures do not guarantee that the event will *not* happen. They are used either to reduce the probability (but not to zero) that the event will occur, or to reduce the cost (but not to zero) of recovery should the event occur. The cost of implementing the protection method should not be greater than the reduction in the exposure rating. Otherwise, more will be spent for protection than the protected resources is worth.

For example, in the case of fire detection methods, they are implemented so that the first can be identified and extinguished quickly, which will reduce losses. In this case, potential losses are reduced but the probability that the event will occur is not reduced.

When the protection method is used to prevent embezzlement, the goal is usually to reduce the probability of occurrence. Thus, this protection method operates on the other factor included in developing the exposure rating.

Security Implementation

After the exposure ratings have been established and the costs determined, the security team should be ready to supervise the implementation of the security plan by operating personnel. The implementation effort will require the coordination of many different groups in the organization, including physical plant personnel, programmers, accountants, and others.

Many of the protection methods may be shown to be cost effective, but budget constraints may preclude the implementation of some. Therefore, the security team must determine which measures require immediate implementation and which can be postponed. Clearly, measures which were postponed should be put under constant review for implementation at some later date.

Exposure ratings and budget constraints are not the only determinants of which measures to implement. Various types of threats will have different internal and external effects on the organization depending on its management structure and philosophy. The security team must consider these effects in selecting the measures to implement.

When security measures have been selected for implementation, it will be necessary to develop a security philosophy among all employees. They must be convinced that the measures are being instituted to aid in the overall operation of the firm rather than to make the working environment more difficult or just to "watch over them." It is important, then, to enlist their aid to ensure successful implementation.

Review Process

After the security plan has been instituted, the security team should not be disbanded as might be the natural tendency. Rather they should meet regularly to discuss how well the security plan is operating, to

evaluate security breaches that have occurred, and to determine what security measures are necessary for proposed data processing applications. Also, they should strive to achieve additional funds for future implementation of other cost effective protection methods.

In addition to their review functions, the internal audit staff should frequently audit the security plan employing standard audit practices as well as attempting to make surprise attacks in the computer system. Because of this responsibility, the audit staff might need to be trained in data processing procedures, computer programming, and computer operation.

The review process is necessary to maintain an adequate security level. First, it is used to ensure that measures already implemented are working as designed. Second, its continual function will ensure that no problem areas are created as more applications are added or modified that those will be included in security plans.

To ensure that the review process is being carried out, a security officer should be appointed. This person could be the original team leader or another who is conversant with security matters. The security officer should be kept informed of new computer applications, plans for acquiring additional computer equipment, and all security violations. Depending on the size of the organization and the potential impact of security problems, the security officer position could require an individual's full- or part-time attention.

MANAGEMENT RESPONSIBILITY

Security is only effective if the plan is well constructed, the staff is committed to making it work, and an adequate review process is established. However, one other ingredient is necessary. That ingredient is management commitment, without which the security plan is destined to failure.

As previously pointed out, implementing an effective security plan requires a great amount of time and energy on the part of the team members. Therefore, a portion of their other responsibilities will have to be delegated to others to ensure that the task is accomplished. Management must be aware of these manpower needs to fully support the plan.

Clearly, to obtain this commitment management must be aware of the economic benefits of both planning for security and implementing security measures. Implementation is easier for management to understand than planning; therefore, it is advisable to do some initial planning to demonstrate the costs and benefits to be derived from a sample of protection procedures.

As security is not a one-shot operation, it is necessary to be quite honest with management and refrain from making promises that cannot be kept. By so doing, the security team will maintain its credibility and be more likely to obtain future funding to improve the security plan as needed.

Robert Courtney of IBM likes to quote from Lewis Carroll's *Alice in Wonderland* when showing the necessity for effective security planning. Alice asked the cat which road to take and the cat replied by asking where she wanted to go. Alice then replied that she didn't

know where she wanted to go. "Then," the cat said, "any road will get you there."

For effective security planning any road will not get you there. But, an effective security plan with well defined objectives will tell you what road to take. The key, then, is knowing where it is you want to go.

An effective security plan protects the computer, the data it contains and the programs that direct its action from accidental or deliberate destruction, modification, or disclosure. The methods of establishing computer security are explicated here.

Leslie D. Ball, Assistant Professor of Quantitative Systems joined the ASU faculty in 1975. He earned the Ph.D. degree at the University of Massachusetts. Steven D. Wood, Assistant Professor of Quantitative Systems has been a member of the ASU faculty since 1975. His Ph.D. degree was earned at the University of Wisconsin.

[From *Datamation*, January 1974]

COMPUTER SECURITY—A SURVEY

(Peter S. Browne, General Electric Information Services Business Division, Rockville, Md.)

ABSTRACT

With the growing requirements for protection generated by legislation such as the 1975 Privacy Act, the increasing complexity of computer and data communications applications, and increasing awareness regarding computer vulnerabilities, the discipline of computer security is achieving independent recognition. Current data processing literature is a rich source of information. Articles and papers regarding security, design of software protection, operational practices and auditing number in the thousands. Most of them are very narrow in scope or so general that they are of little use.

It is important to the data processing professional to be able to sort out the large body of material in order to gain perspective. This paper attempts that by relying on a carefully selected and fully annotated bibliography of 133 items, many of them of interest to the systems analyst or designer. These papers are referenced in the text, which attempts to carefully distinguish between the technical and operational elements of computer security, while providing an overall perspective.

INTRODUCTION

The computer has unleashed countless opportunities for industrial growth, activity, new applications, labor-saving accomplishments, improving the quality of decisions and many others. Most industrial and governmental organizations could not survive without the processing capability of their computer systems, and it can be shown that society itself is dependent upon the computer.

At the same time, computer technology has spawned a whole new field of crime and generated a series of problems for both designers and users of information systems. A perusal of some of the better publicized horror stories will attest to this situation.

With the growing pervasiveness of computers, their increasing complexity and the development of sophistication regarding computer vulnerabilities, the discipline of computer security is achieving independent recognition. Many organizations have created the position of DP security specialist or manager and college courses in computer security are being taught. There are a number of driving forces behind the interest, and some of them are outlined below.

Historical

In the middle 1960's there arose in Congress discussions over the issues of privacy and the computer. A national data bank had been proposed and the public testimony in Congressional committees fills a number of books. At the same time, the general consensus was that technology had not advanced to the point where any semblance of privacy could be maintained.

However, the concern over the inherent lack of controls in computer systems led to much discussion and some activity on the technological front. A landmark meeting of most of the active professionals in computer security in 1972 set the stage for an understanding of the technological issues and led to intensive design efforts to achieve "secure" computer systems.

In the meanwhile, activity on the legislative and social fronts saw a culmination in the Privacy Act of 1974 (Public Law 93-579). This act applied privacy requirements to most computer systems operating within the Federal Government. It also generated a number of papers regarding implementation requirements, and some effort towards determining the true cost of privacy, especially as applied to large, multi-use data banks.

The need for computer security is also driven by technological factors. As systems become more complex and sophisticated, so do the problems of data integrity. Resource-sharing systems achieve their greatest advantage when used simultaneously by many customers. This also means simultaneous processing of data with varying needs for confidentiality and pervasive needs for accuracy.

The problems of control also have increased as the flexibility and capability of systems improve. With many users on-line at one time, system crashes become more serious and the entire operation becomes more complex, therefore subject to error.

This paper will attempt to survey the technical aspects of data security. The scope and complexity of the field becomes apparent when a survey of the literature turns up over a thousand articles dealing with physical security of computer assets, threats to the computer, protection against fraud, embezzlement, and other human failings, the need for insurance, software protection, hardware safeguards, legal aspects, risk assessment, auditing, computer system design and the principles of operating system software security. Needed, then, is a multi-disciplinary approach.

Definitions

Although computer security is a widely discussed subject, and a generally agreed definition refers to it as protection of data against accidental or intentional disclosure, destruction or modification, it can refer to many different things. It has in the past meant the protection

of computer systems from attack or destruction by a variety of threats, ranging from natural disasters to acts of dissident groups. Security can be viewed as a problem of "comprehensive control," involving the development of means to insure that privacy decisions are enforced.

Data confidentiality is a guarantee to the proprietor or subject of computer stored data that the information contained therein is not made available to unauthorized users. It refers to the protection of data from unauthorized disclosure, whether the basis for such protection is agreement, law, policy or prudent judgment.

Privacy is a legal and social concept, having roots in constitutional law and social justice requirements. It refers to the right to data confidentiality.

Data integrity is the protection of data against accidental or intentional destruction or modification. It is the ensuring of accuracy and completeness. It involves the need for all components to operate together in a consistent and reliable manner.

It can be seen that the object is data. Therefore, we have been discussing data security as contrasted with computer security. To include the broader-based definition of the subject, and the need to think of the other assets involved such as computer hardware, facilities and people, the term 'processing integrity' has been coined. It is the property of having adequate processing capability, availability and reliability in order to provide the requisite service of data processing.

PLANNING FOR COMPUTER SECURITY

Threats and vulnerabilities

The result of a security breach is what usually draws attention to a threat, a vulnerability or a particular countermeasure. Thus, we find that the short history of computer security is spotted with numerous "horrible examples," fads such as the interest in magnets as a threat and implementations of security measures that are anything but cost-effective. A rational approach to the subject implies some sort of quantification of risks, countermeasure costs and the benefits to be derived from implementation. Though numerous articles and papers have called for this approach, only recently has there been a serious attempt to model the risk-cost interface.

One of the key steps in devising protection is that of the classification of various threats. There are two sources of threats, people and natural hazards. It is possible, though not easy, to quantify the threat of fire, earthquake, flood and storm. On the other hand, those events that arise from human acts such as mistakes, disgruntlement, fraud and sabotage are not always possible to quantify, namely because of the complexity of motivations, and the strong effect of the environment, the target and the countermeasures imposed. The first step is to organize and classify the threats in a systematic manner.

Threats are usually given as part of the environment. On the other hand, the vulnerabilities of a particular computer system or installation to those threats are very much dependent on a large number of factors, relating to location, people, capabilities of the system, building structure, nature of the processing and operating practices. Most security surveys and evaluations are designed to review these instal-

lation dependent vulnerabilities and postulate countermeasures accordingly.

Providing adequate protection against threats to the security of data in a cost-effective manner is not generally found in practice. The reason is that in too many cases, the implementation of computer security is relegated to a minor spot in the organization. Also, because of inadequate analysis and lack of a systematic approach to computer security as a management problem, too many existing measures lack flexibility, consistency, completeness and redundancy. These attributes are all necessary in order to achieve protection that works when it is supposed to. One hundred percent security or reliability is never possible. What is needed is a set of security measures that take into account the failures, errors, omissions and vulnerabilities of any given environment.

Risk analysis

Risk analysis is the term applied to the quest for systematic quantification of threats, loss exposures and countermeasure benefits. The ingredients of a risk analysis are the postulation of threats and their probability, the calculation of loss of assets or productivity that can result from the imposition of threats, and the establishment of loss potential thresholds, usually on an annualized basis, that the organization must attempt to lower by the addition of security countermeasures. Numerous methodologies exist. Some of them consider only the application and data file viewpoint and others consider all the assets that are part of the data processing environment. The basis of the methodology is the same. It is to estimate the loss that can arise in different manners and on different assets as a result of a threat, each time it occurs. The result is usually postulated on an annualized basis (number of threat occurrences per year times the average loss per occurrence). The result can be used to compare against the cost of countermeasures that will reduce the threat probability or will lessen the expected loss that would occur. Caution must be exercised to not ignore the very low probability, high loss events that occur so infrequently that the annual loss potential appears negligible. In any event, the apparent simplicity is misleading. It is not easy to quantify all the losses, to postulate all the threats or to determine their probability, especially since the particular environment plays such a large part. It is also a complex and time-consuming task, which accounts for the relatively few completed risk analyses to date.

OPERATIONAL COMPUTER SECURITY

Computer systems are generally not designed with security as a primary objective. Generally, the large main-frame manufacturers claim that users have been slow to request this security. Yet the large interest in the field, and the amount of research effort by independent sources and manufacturers alike indicate that the next generation of computers will achieve adequate, measurable and certifiable protection in hardware and software.

Most opportunities to devise protection for computers do not fall in the lap of system designers. The people who manage the world's existing computer installations are largely concerned with the problems

of system integrity, processing availability and security. For them, much of the literature that deals with physical security, backup and administrative controls as applied to computers is highly relevant.

Physical security

Physical security is perhaps the most mature element, having been subject to study and implementation long before computers. Implementation of physical access controls to computer facilities represents a generally agreed first step in achieving threat protection. The reason is that many threats, especially of a human nature, can be reduced by limiting access. To deal with the threat of fire, utility unreliability and environmental disturbances, numerous control and monitoring systems have been devised. All should be considered in the context of the overall DP security plan, even though responsibility for their implementation may be elsewhere in the organization.

Backup and recovery

Adequate recovery planning to ease the pain if a disaster were to strike is important. Recovery planning implies that first the organization has to be able to respond in case of emergency. Then the off-site availability of supplies, data files, programs, documentation and equipment must be considered. Finally, there must be a plan in place so that in case of disaster, all the elements can be pulled together in order to resume operations in as short a time as possible.

Administrative controls

The administrative burden of proceduralizing and formalizing a security program is generally underestimated. It takes great clerical resources to ensure adequate maintenance of a selective access program, whether it be selective authorization to data files or physical areas. Organizations should be prepared to commit at least two full-time persons to the job. Other administrative aspects include the development and implementation of security policies, guidelines, standards and procedures. Again, these functions may be centralized or decentralized, but stand a greater chance of success if the latter.

Security in recent years has been a major concern of computer operations groups. It is here that the organization can channel resources most effectively to deal with the lack of security in operating systems or in application system design. It is the last resort, or to put it in a better light, the necessary but not sufficient condition for providing true computer security. One of the best guides for information about various operating practices is the System Review Manual on Security published by AFIPS. Other guidance can be found in the more exhaustive of the many checklists and guidebooks on providing computer security.

Audit

Audit has been defined as "an independent and objective examination of the information system and its use (including organizational responsibilities) into the:

- Adequacy of controls, levels or risks, exposures and compliance with standards and procedures
- Adequacy and effectiveness of system controls versus dishonesty, inefficiency and security vulnerabilities."

Independent and objective are the key words, whether or not an auditor has as the objective of his review the detection of fraud in computer systems, his role is certainly one of reviewing the adequacy of system security. Many CPA firms have finally recognized their unique role in security assurance. There are those who say their attention is still inadequate and not yet relevant. Suffice to say that computer systems need auditing, both internal and external. It is not possible to even consider auditing "around the computer" because of the risks involved. Given the nature of computer related threats and vulnerabilities, the traditional independence and inquisitiveness of the audit profession and the requirement for independent assessment of controls, it is logical that much computer security activity will be a part of the auditor's domain.

TECHNICAL ELEMENTS

Even though the first line of defense is to rely on secure operational practices, the elements of system design have always intrigued computer security professionals. The people who manage the world's existing computer installations are largely concerned with how to improve operations and achieve a better means of security. For them, most of the literature that deals with physical security, backup and administrative controls is highly relevant. Here the word "design" implies the development of a viable computer security program that is adequate, but not confining, and one that is limited to operational viewpoints.

Obviously things can go wrong with hardware and software. Data integrity, encryption and measurement must be considered in any complete computer security program. Understanding of these elements usually requires a person well-versed in systems programming and application system design. That the skills required in this area are completely different (and perhaps incompatible) with the skills required for handling operational security problems has not been well postulated in the literature.

Identification

Positive identification of people, devices, programs, items and processes is clearly a requirement for adequate security. Holding a person accountable for his actions is one of the first principles in good design. This requires certain knowledge that he is who he says he is. There are three approaches to personal identification, (1) identification based on passwords (2) on credit card technology and (3) on personal characteristics of the requestor. Passwords are the most common method, but they suffer from some serious inadequacies. They should be random in nature and of sufficient length to avoid compromise. They are usually anything but. The use of credit cards, usually with a magnetically encoded stripe, is achieving great popularity, especially in regard to EFTS. This approach makes sense if the cards are controlled, used in conjunction with a unique personal identifier (PIN number) and if the system is made aware of lost cards so that casual retrieval of a badge will not be an open invitation to access. Identification based on personal characteristics, such as voiceprints or fingerprints is still not a commercially popular methodology, but offers the most promise for the future. Identification not only relates to personal access, but also

to other system entities. Security objects can be people, terminals groups of people (cliques), programs, terminals, data communications devices or segments of virtual memory. Then one can specify restrictions based on a number of parameters such as the characteristics of the requestor (name, terminal, program, etc.) content of data (all salaries over \$30,000), context of data (association of college grades, number of parking tickets and credit rating) or one can use procedures (formularies) based on the nature of the situation.

Authorization

Once a system resource or person is identified, the problem of access of the identified subject becomes an important concern. Authorization refers to the establishment of which interactions among system elements are possible or allowed. The traditional concept of authorization in system design presupposes that any system entity automatically is authorized access to any other system entity unless specifically prohibited. The secure concept of system design takes the opposite view. the concept of "lease privilege" holds; namely that any system entity is prohibited from access to another system entity unless specifically authorized. For example, there is no need for a peripheral allocator to be able to control or even have access to user data bases or other elements of the operating system. It should have knowledge of only those resources necessary for allocation of devices to jobs.

The concept of an access matrix espoused by Conway, et al. appears to be the easiest way to implement access control, but the implementation is not clean. There are a number of choices that one can make in defining the rules of access. For example, what level or degree of privilege should be permitted? Are we talking about control of access to files, records, elements within records or specific hardware or software elements of the computer systems?

Much of the early work in authorization technology is the result of research activities. The academic environment has fostered some good studies which have led to some actual efforts at implementation. Work at MITRE and the US Air Force on security kernals (provably small security reference monitors) as Stanford Research Institute on proofs of program correctness. at System Development Corporation for the DOD community, at MIT under Project MAC and at computer system manufacturers, has led actual demonstartion of computer and communications systems with security as a prime design requirement. An excellent but dated paper by Saltzer summarizes current (as of early 1975) research and development efforts.

Integrity

Obviously, things can go wrong with hardware and software. Data can be (and frequently is) inconsistent or unreliable. Data integrity interfaces with computer security at almost every point. In fact, many observers see the two concepts as being nearly synonymous. A high integrity operating system can by its nature provide security against unauthorized use of system resources. System integrity is the condition of proper and predictable operation of the total system, including hardware, software and human elements. It includes the physical and operational security mechanisms in place.

Part of the integrity solution lies in providing an operating system that does not treat every operation as "benevolent", but in fact as-

sumes that users are going to attempt to get into supervisor state, and are going to overreach the limits of the software design. Other corrective elements can be found in attempts to enhance the reliability and availability of applications.

System audit trails

System surveillance, measurement and auditing are critical elements in providing the technical base for adequate security and integrity. The effectiveness and operability of the entire system, and especially of the protection mechanisms must be continually scrutinized and measured. Management must be assured that the protection is in place and effective. Management must also be able to detect and to respond to events that constitute system security threats. Many of the same mechanisms used for performance measurement can be used for both the monitoring of the protection mechanisms and the integrity of the entire system. A properly functioning audit mechanism should allow the specification of certain system events (such as OPEN, LOGON, etc.) to trigger an audit trail. The interfacing of system measurement and surveillance activity with the auditor is the subject of much activity and research.

CONCLUSION

As of early 1976, systems are in use which provide a high degree of computer security and integrity, and may provide the basis for systems accreditation. The MULTICS project at MIT has led to commercial marketing of the system by Honeywell and a multi-level security enhancement by MITRE and the USAF. The General Electric Mark III service has long been known for its good security, and can claim never to have been penetrated. Other operating systems have been designed with security as an objective, and the efforts of IBM and Honeywell have been previously mentioned. Current research directions are outlined in the paper by Saltzer and should see the light of commercial reality sometime in the next few years. Awareness of the risks is being fostered by numerous seminars and conferences. Large organizations, both commercial and government, are funding the position of systems security officer or computer security manager. An association, the Computer Security Institute, has been formed to provide information to, and give voice to the growing number of specialists in the field.

Current state of the art would seem to allow quite flexible and cost-effective security measures. But in practice, protection is generally not elaborate, flexible or impenetrable. As a result, most safeguards are imposed "after the fact", by mixing managerial controls and physical security. Most of this type of control is ineffective, due to inconsistencies, lack of proper redundancy or incompleteness. It appears that this will be the case, even after computer systems come provided with flexible and effective protection mechanisms.

In 1969, Lance Hoffman said that much research is needed to design security controls and to evaluate computer access control methods. Nothing has changed to alter this. When designers and implementors agree on the needs, and the computer and software providers supply the secure methods to use their products, it is still up to the user to

provide the proper environment, the procedures and the management climate to implement the principles of "least privilege," compartmentalization, redundancy in controls and personnel awareness that are the necessary first step in provision of security, privacy protection and system integrity. Only then, shall we realize the goals of simple, economic, functionally capable and modular protection mechanisms.

In conclusion, it is important to realize that we are talking about a complex technology, with many interfaces. Because of the great need, the next few years should see a broadening of interest, the forcing of computer security protection because of privacy legislation, awareness of the economic consequences of security deficiencies, increased risk management efforts by computer system implementors and increasing government regulation of the data processing industry.

[From *Datamation*, January 1974]

COMPUTER SECURITY—AN OVERVIEW

(By Harold Weiss)

Top management concern about computer security was stimulated recently by several well-publicized cases of computer-related fraud. Most notorious of these is the massive Equity Funding scandal in which insurance policies worth some \$2 billion were fabricated. This was only one facet of an incredible caper that has rocked the financial community. Around 1969 and 1970 there was similar management concern resulting from a rash of bombings of computer centers. In 1972, tropical storm Agnes with its widespread destruction of data centers, also caused a flurry of interest in computer security at the upper levels of the executive hierarchy.

This concern is well-founded since many chairmen of the board have effectively been playing corporate Russian roulette. At any moment their organizations might receive their equivalent of a bullet in the corporate brain. This would result from the almost total collapse of the organization's information system concentrated in and around the centralized data center. A localized fire, an unhappy employee, a storm, or numerous other events could trigger the disaster.

Aside from the catastrophic effects on employees, stockholders, customers, and other elements of the population, top management can expect to suffer personally from legal action if imprudence in security planning is demonstrable. Yet in relatively few companies does one find a resolute attack on the urgent problems of computer security and a commitment of appropriate manpower and monetary resources. Even in these cases, when profits start to sag, security and control are among the first areas to be cut, presumably as "frills."

With or without high level management prodding, the data processing manager must devote high priority to security planning and implementation because the stakes are so enormous. Some of the decisions made could easily cost or save the organization tens of millions of dollars or lead to its demise. In view of this awesome responsibility, the data processing manager should not be making such decisions person-

ally, but should be passing on assessments of the hazards, the costs of security measures, and recommended actions. It is up to higher management to decide the level of permitted risk, to assure that it is acceptably low and at reasonable cost. They must be convinced that recovery will still be possible and relatively efficient.

In addition to the primary security concerns, which are survival of the organization and preventing the destruction of major corporate assets, attention should be given to the integrity, accuracy, and validity of the organization's information system; the prevention of large-scale computer-related fraud; and needed privacy of proprietary data.

The broad nature of the computer security problem will be explored in this article and some recommendations made to data processing managers. Disaster-level problems will be emphasized.

EXPERIENCE WITH DISASTERS

If one collects incidents of computer-related disasters, as I have done for about a dozen years, it is quite easy to go overboard and become a security nut or be obsessed about control requirements. As with all aspects of computer work, compromise is necessary. We must strike a balance between the need for various kinds of protection, the cost, and the interference with the operation of a system. It is possible to quality-control a manufacturing plant so tightly that nothing ever gets shipped or product cost becomes prohibitive. Similar considerations affect the information factory. The very first truly commercial application ever placed on a computer failed because, among other reasons, excessive controls and constraints placed upon a payroll system made it unworkable. So, security, while a major concern, should not normally be an overriding one in commercial data processing installations.

Data centers have proven to be very fragile things when one reviews the wide range of incidents that have destroyed them or seriously interfered with their functioning for prolonged periods of time. Fire, water, and malicious acts by people pose the worst threats of serious damage or destruction. The last statistics I saw showed about 2½ million fires reported annually in the United States. Other data indicate that probably over a million of these are to buildings. Inevitably, some of these building fires affect computer centers each year. The first large-scale computer disaster was the Pentagon fire in 1959. In July 1973 the Army Records Center in St. Louis experienced a very large fire that did extensive damage for which they were ill-prepared. IBM was the recent victim of a large computer fire apparently caused by arson.

Water damage to computer centers has occurred from numerous sources. Tropical storm Agnes was the worst offender. It was estimated that hundreds of computer systems were buried under tons of water and mud in the Middle Atlantic section of the country. In 1970 hurricane Celia caused devastating problems for many computer users in Corpus Christi, Texas. In addition to hurricanes, water damage to computer centers has been experienced from floods, the activities of firemen on higher floors, broken pipes, sprinklers, water mains breaking, sewers backing up, underground streams, and leakage in the computer's water cooling system. In the Army Records Center fire, water damage was much worse than that resulting from the fire itself.

Malicious acts by people are becoming more significant factors. A few years ago there were 4,330 bombings in this country in a 15½ month period. Several of these were of computer centers, particularly at universities. Such incidents also occurred in Canada and Mexico. A computer operator is reported to have physically sabotaged his company's computer at least 56 times in a two year period. Striking maintenance employees of a computer manufacturer allegedly sabotaged a customer's data communications network in a harassing action. I have been told of several sabotage actions by recently terminated data processing employees and of several cases of program sabotage, but these have not been verified to my satisfaction. In any event, this is a growing area of concern. The computer is a symbol of mechanization and automation; hence, it becomes a primary target of disaffected elements in society.

Other events which have taken out computer centers include explosions, an earthquake, a tornado, aircraft crashes, extended loss of electric power, strikes, war, lightning, serious equipment malfunction (eleven days of cpu outage at one installation), air conditioning breakdown, industrial chemicals or gases, sandblasting near the air conditioning intake, steel wool (two data centers), even hair spray sucked into a computer's air conditioning system. Anyone wanting to research the problem need only scan the front pages or newsweeklies for the past four years. Many of the incidents are never reported in the press, however. Neither the victims nor the computer manufacturers are interested in this type of publicity.

Computer-related fraud merits special attention. Normally, this is not as potentially catastrophic an even as some of the hazards listed above. In the first 15 years of business computer applications, very few frauds surfaced and few of these had significant impact on the organizations affected. In the past few years, as computers proliferated and computer knowledge became more widespread, and perhaps because of changes in morality, computer fraud has become more prevalent. The size of the losses in a number of recent cases has become great. In addition to the huge losses resulting from the Equity Funding fraud, there have been several more cases in the million-dollars-and-up class and numerous lesser frauds have also been disclosed. One must be careful in reviewing reported incidents since many apocryphal stories keep circulating. Also, some ostensibly computer-related frauds turn out to be true frauds, but not true computer crimes. There is a feeling in the auditing profession that this is only the tip of the iceberg—that many more computer-based frauds have been uncovered but not publicly disclosed, and an even larger number remain undiscovered.

RECOVERY REQUIREMENTS

Since more and more of the critical information assets of an organization are being concentrated into a smaller and smaller physical area, the results of a localized computer disaster can be catastrophic. The computer is no longer a useful adjunct of business operation, an oversized bookkeeping machine, but a vital part of daily operations. The informational life blood of the company pumps through the corporate computers and relatively brief shutdown of the machines or loss of key machine language files and programs will quickly shut down a business.

To illustrate the critical nature of this problem (the bullet in the corporate brain previously alluded to), I shall take you through the recovery process assuming that your computer room and adjacent work and storage areas were destroyed by a fire or an Agnes-type burial under water and mud. I shall also assume that what are considered good computer center practices were followed. I shall try to establish that even these are grossly inadequate.

In order to recover you will need:

1. *A compatible computer or computers* (including essential peripherals, any special hardware or equipment options, terminals, data communications equipment, etc.).—Backup facilities, while desirable, are becoming less and less realistic. Recovery will not be feasible until a large volume of computer time is available on compatible equipment. This means, in most cases, after you have gotten replacement equipment. How long might such replacement take? This might be weeks or months. In practice, the vendors, although refusing to be contractually committed, have recognized the customer's crisis and have done a magnificent job of rapid resupply. Each case, however, is a unique problem and the vendor may not be able to react rapidly because of factors not under his control.

2. *Programs* (both applications and key systems software).—There is a possibility that programs kept in a safe or vault near the data center might survive the disaster. Remotely stored programs tend not to be absolutely current. We cannot pay people with obsolete or illegal procedures, for example. We need to know what changes should be made to perhaps hundreds of remote programs in order to make them current. Any program requiring change will then need to have test data developed, the changed programs validated, and surviving documentation (if any) revised. A considerable amount of computer time and calendar time may be consumed to accomplish this, if it can be done at all.

3. *Master files*.—Again, good practice would require retention of key master files in secure safes or vaults and/or at a remote location. The only thoroughly reliable source of backup is the remote copy. Usually this is the grandfather generation of a file; a snapshot of a ledger produced three processing cycles back. It is unfortunately the son or current generation of a file which needs to be updated during the next processing period.

4. *Transaction files*.—For each application master file that survives, you need all the transaction files subsequent to that generation in order to become current again with that single file. It may take huge amounts of computer time to process forward even two generations with a large file. If the transactions are not in machine-readable form, the recovery problem is greatly complicated. We want to go back as little as possible in each processing cycle to accomplish recovery. In a sequential system, edited and sequenced transaction files should be the ones retained. To come back two generations for a large number of master files becomes an almost impossible task. Also, there is the additional problem of the destruction of current transactions awaiting processing at the time of the catastrophic event.

5. *Know-how*.—To recover efficiently after a data center disaster takes documentation. In addition to the knowledge of required pro-

gram changes discussed in the second category above, we need to have key systems, programming, and operations documentation survive the catastrophe. Presumably, user documentation will remain, given the localized nature of the disaster which I have postulated.

6. *Ancillary facilities and services.*—This includes an appropriate physical site, power, environmental controls, etc. In a number of incidents air conditioning was the limiting factor for recovery.

7. *Forms.*—The special forms the organization uses must be on hand. Vast quantities of forms were lost in tropical storm Agnes. With the developing shortage of paper, rapid resupply may not be possible. It may be wise to stock an emergency supply of critical forms at a remote location. One utility estimates that it would take a railroad freight car to hold the forms urgently needed for a week's backup operation.

8. *Skilled personnel.*—Hopefully, key computer staff will survive the disaster, although they are particularly vulnerable to a bombing. Since recovery from a disaster may be very arduous, some of the less loyal members of the computer staff may decide to depart at this time. Experience indicates that in the event of widespread physical disaster, such as a hurricane or earthquake, needed computer personnel are initially tied up with family and other personal problems.

PLANNING FOR RECOVERY

A little calculation by the data processing manager of almost any organization extensively utilizing computers will indicate the total unreality of attempting to recover from the type of computer area destruction which I have described. Recovery planning is really set up to recover from relatively minor problems—the brief machine outage, the need to re-create one generation of one file from one application, the need to restart from a system crash, etc. Many disaster plans do not provide for all the ingredients necessary for efficient recovery, hence will fail if and when the moment of truth comes. It is, of course, totally unrealistic to attempt to come back from true disaster by means of large amounts of hard copy or microfilm. The information in programs and files must survive in machine-readable form. Fallback to manual or other prior systems is also not practical in most cases since the current volumes tend to be much greater, the required people and skills lacking, the written procedures gone or obsolete, the old bookkeeping or unit record machines extinct, etc.

What, then, would happen if true computer disaster strikes the heavily-dependent computer user? Would the organization shut down for a lengthy period of time until adequate computer service was restored? Would a fantastic backlog of transactions be piled up, awaiting restoration of service to a normally heavily loaded facility not capable of doing much catch-up? How efficient would your organization be during this recovery period? Would you retain your customers? What would happen to your cash flow? What would recovery cost, if still possible? I believe many organizations would be hard-pressed to survive this traumatic experience. Certainly, the chief executive should be given these facts of life before investment decisions are made regarding computer security.

A VITAL RECORDS PROGRAM

What is needed to protect the organization then is assurance that current copies of all essential computer programs, files, and documentation will survive the serious disaster. Even safes and vaults on-site cannot provide sufficient protection. What is required is the storage of the most recent duplicates of machine-readable records and programs at a highly secure remote location. This location should be kept confidential and known to only a few of the most senior employees.

The cost for this protection is not exorbitant. Magnetic tape, the usual retention medium, is very inexpensive. With an available tape drive, key sequential files can be written simultaneously to two drives, in order to provide the backup copy. If this is not feasible, multi-programming permits file duplication without excessive burden in view of the significance of the protection. On-line files and programs can be dumped daily to tape. What is critical here is the location and other aspects of copy storage. Data communications facilities, if already available, should be considered as an electronic solution to the logistics of distribution. Regularly available courier service, such as to a bank, the intra-company mail, or the U.S. Postal service, may also provide low-cost shipment and return of vital media (although some methods may not provide sufficient security).

The hard part in a vital records protection program is deciding which records, programs, and documentation are essential to survival, and working out the mechanisms for handling the logistics and the necessary security. The operation of the plan should become routine. Experience, however, indicates that practices tend to deteriorate with time. Someone must be given the responsibility of administering the vital records program and providing quality control. The program should be occasionally reviewed by the internal audit staff to see if it is functioning as planned and in conformity with management directives.

REDUCING THE RISK

In addition to the critical requirement of designing efficient recoverability into the organization's data processing activities, a number of steps can be taken to greatly reduce the risk of disaster and the cost of recovery. For example, planning for security should take place early in the system design phase, not as an afterthought. Logically, priority should be given to the most hazardous risks and to the lowest-cost solutions.

There is no totally secure computer installation. This is not technically or economically feasible. Practical solutions, however, are possible and a number of organizations have achieved relatively secure systems at acceptable levels of cost. Clearly, the size of the processing facility is a primary factor in the planning. (It is difficult, for example, to get a good division of duties when the technical staff consists of one person.)

Consider these things in reducing the risk:

1. *Physical location.*—A wise choice will greatly reduce many hazards. Computers have been located at airports, over garages, boilers, paint shops, in old wooden warehouses, basements, store fronts, on

campuses, in earthquake-prone areas, in heavy traffic areas of office buildings, and other such choice sites. If a vulnerable site must continue for the present, steps can still be taken to reduce the vulnerability; for example, where water damage is a high risk, you can store media as high as possible, provide drains, pumps, emergency power for pumps and fitted plastic covers for equipment, and seal utility outlets.

2. *Physical access control.* This has received considerable attention at many installations, but I find serious deficiencies and token protection. Badges are not checked carefully; locks are taped open or released without adequate investigation of the visitor; security is lax at night or weekends; the facility is wide open and unsupervised during the weekly heavy cleaning period, etc. *Nobody* and *nothing* should be permitted into the computer room unless they or it needs to be there *then*. All legitimate visitors should be accompanied by a staff member. There should be as few windows and doors as feasible. Normal access should be via one tightly controlled entry point; other doors should have alarm devices on them—a wide range of devices are available for access control, including use of a computer for this purpose. The key defense, however, should be an alert computer staff which will immediately challenge all strangers who gain access by whatever means. Physical access control should include bomb protection against packages and mail which should be opened outside the computer center.

Control of access to remote terminals is increasing as a problem.

3. *Fire protection.*—Fires don't usually originate in the computer room. Consequently, the data center should be located so as to minimize external fire hazards. The room construction should be of flame retardant materials. The amount of combustible materials in the computer area, such as paper stock, should be minimized; cleanliness is vital in providing a noncombustible environment. An early warning fire detection and quenching system should be backed by small portable extinguishers spread around the computer area (and personnel should be trained in their use). A separate air conditioning system for the data center is recommended. All emergency procedures should be in writing and personnel should be thoroughly drilled.

4. *Media protection.*—A misconception should first be cleared up: there is no precise figure, such as 150° F., below which magnetic media are safe or above which they are destroyed. However, the degree of humidity is quite significant. High humidity can cause serious media deterioration without great temperature elevation and, conversely, at low humidity levels considerable temperature elevation may not result in serious damage. Up to about 125–130° F. at normal humidity levels in data centers few problems are encountered. As the temperature is raised, a gradual increase in the error rate on reading magnetic media will be experienced. Over 150° deterioration becomes more rapid. There is also a lower limit of temperature tolerance. I heard of an incident in which an accounting firm ran into trouble with a portable audit retrieval system on a disk pack by leaving it in a car trunk on a very cold day. Another misconception is vulnerability to magnets. Magnetism is a very weak force which falls off very rapidly with distance. A magnet has to be very powerful or extremely close to the affected surface in order to cause a problem.

The organization's vital records program should lead to a "vital" classification for many programs, master files, transaction files, and

related systems documentation. They merit top protection. A separate room is desirable for storage of this valuable property with very strict access control. If possible, a librarian should be constantly responsible for these media. Media should be released just before use and returned to secure storage immediately after use. The records management system must be periodically reviewed to make sure it is working properly (in one company, managers discovered that people were getting into a locked media library during "non-working hours" through a false floor).

Smaller organizations should also consider vault or safe storage with sprinkler protection. Exposure to water is not damaging to magnetic media for short periods of time.

5. *Computer fraud and internal control.*—We are primarily concerned about computer-related fraud, where use of the computer was either a significant factor in perpetrating an embezzlement or otherwise increased the company's vulnerability to fraud.

Some types of fraud, such as those that require altering many balances, are more easily perpetrated on computers: Equity Funding is a prime example. Illegal revaluation of an inventory, another type of fraud involving small-scale skimming of many accounts, has been called the "salami" fraud. A few cents taken from many accounts is placed in an account controlled by the thief. With magnetic storage there may be little obvious evidence of tampering.

To put matters into perspective, despite several recent well-publicized incidents, including the Equity Funding case (which has resulted in the indictment of three computer professionals), computer fraud is not comparable in hazard to many other potential disasters. A fire, an earthquake, a tropical storm is much more likely to cause serious computer-related damage to your organization. Computer crime is increasing, however, both in frequency and in the magnitude of individual incidents; hence it will be of growing concern to data processing management. Despite a flurry of concern when Equity Funding and other frauds were publicized recently, most top executives are not likely to take the steps necessary to really deter further dp crimes, such as investing in a strong computer audit function. Security costs money, and we must overcome the feeling that a disaster "can't happen here."

There are several steps that can be taken to improve internal control and reduce the hazard of computer fraud:

a. There should be a division of duties in data processing. It is desirable to separate programmers, operators, librarians, data preparation staff, and data control personnel. Separation of developmental programming from maintenance programming is also helpful. If possible, at least two people should work on a project. Operations personnel can be rotated on duties. There should be restricted access to the computer, programs, machine language files, documentation, and sensitive forms, such as checks. Many data processing installations are much too lax in this regard. In a number of cases, including Equity Funding, much of the hanky-panky was done on weekends.

b. Systems need built-in controls. Where feasible in sensitive areas, external controls should be maintained by parts of the organization independent of data processing. It is useful to know the dollars to be accounted for, the number of people to be paid, to have a hash total

on pay rates, etc. Terminals should be under strong programmed control. There should be well controlled error handling procedures.

c. There should be control over file and program changes. Authorization and review should come from outside data processing. It helps to have a software librarian to preserve the integrity of the program library.

d. A security specialist can be appointed in data processing, particularly when complex on-line systems are involved.

e. There need to be strong audits of the data processing function by both internal and external auditing and apparently weak external audit of the mechanized systems. The auditors reportedly never dealt directly with the data processing staff at Equity.

6. *Backup and "fall back" capabilities.*—Even a little backup computer time in an emergency can be very helpful. The small user of a common configuration has less of a problem. I know of a case, though, where a company could not formalize a reciprocal backup arrangement with any of sixteen apparently compatible equipment users. This formalization is essential and should be arranged with several users, if possible. The technical problems associated with equipment, and to a lesser extent, software compatibility, are often severe. Also, appropriate communications need to be arranged. If compatibility is achievable with an interested organization, the real crunch will be on the amount of backup time available. Backup must be tested initially and periodically thereafter. Backup is more secure if arranged internally in a large organization; some companies are paying regularly for options on emergency processing time. Others have contracts with cooperative service bureaus to assure the availability of backup time. Different industries have different peak processing periods in the day or month and beneficial arrangements can be made with the right kind of partner. It is safer if the backup facilities are not subject to the same hazards (earthquake, power loss, etc.) as the primary facility.

As to "fall back," some organizations can allocate jobs to smaller, compatible machines in a disaster. For short emergencies manual procedures may be possible. Certainly these alternatives should be explored, and well in advance of need. Priorities must be carefully evaluated. All backup and fall back procedures should be documented in detail and the computer staff trained in their use.

7. *Personnel.*—This is potentially the weakest link in the security chain. How do you protect your organization against legitimate data processing staffers who have authorized access, but for whatever reason want to harm their employer? Some of these employees, such as the systems programmers, have considerable knowledge, and are involved in esoteric assignments not easy to monitor. There have been numerous authenticated security problems caused by data processing personnel, including physical and programmed sabotage; programmed frauds; theft of proprietary information such as programs, systems documentation, and customer lists; theft of machine time and supplies; and strikes.

Obviously, the best method of risk reduction is better investigation of potential hires for the data processing function and one of the key factors in selection is fitness for jobs of a fiduciary nature. The staff should be bonded. When a data processing employee is discharged, he

should first be immediately removed from the company premises. All company identification should be collected and relevant combinations of locks and passwords changed. Also essential, but sometimes forgotten, is rapid communication of the termination to other members of the staff. There have been several incidents of sabotage when these procedures were not followed.

Voluntary termination of key computer people has been damaging to many companies. Good documentation, cross-training, and more than one person on a project can ease the problem, as can a strong staff development program.

8. *Data processing risk insurance.*—We cannot design riskless computer systems, so investigate the potential for loss reimbursement. In some cases insurance is an acceptable substitute for certain security measures which may be more costly. Insurance helps cover some of the large out-of-pocket losses that may be incurred despite good data processing security. Conventional policies may be used for coverage, but they tend to be too restrictive. Special data processing policies, now written by at least twenty insurance companies, are not an off-the-shelf standard product and require quite a bit of effort to tailor the coverage to a company's needs.

The best security procedures may never be followed because control and security constraints tend to be inconvenient. But there must be policing by management or things will inevitably get lax.

The first level of review should be made by the data processing management. However, this does not provide enough protection for the organization even when a separate control or review function is established within the computer group. Independent review is required. In most companies top management has delegated this assignment to the internal audit staff. (Some financial systems will get examined by external auditors and specialized audits also are made by a variety of government agencies.)

AUDITORS' ROLE

The role usually assigned to internal auditors includes reviewing controls, ascertaining compliance with company policies, assessing the safeguarding of assets, determining the reliability of management information, appraising the quality of performance in carrying out assigned duties, and recommending operating improvements. There is a misconception among some data processing managers that audit of their function is an adverse reading on their ability or prerogatives. The most skilled computer staff in the world should still receive management review. The internal audit staff has been delegated this review function by top management since senior executives cannot perform enough of it on their own in a large organization. The internal audit function evaluates the effectiveness of the rest of the organization's controls, hence is itself one of the most important controls. It is a sign of maturity for the data processing management to encourage and invite review. The internal auditors can reduce the intrinsic high risk of data processing activities, help solve problems, and improve control and security.

Data processing managers are often unaware of serious deficiencies in their operations. Some accept excessive risks as a natural way of life

in computer work. Auditors have found incredible practices even in large companies, such as the computer staff using hand fire extinguishers to cool soft drinks, a four hour rated tape storage area which had a wooden door covered with metallic-looking paint, no inventory control over check forms, media vaults which couldn't be closed, and many others.

More and more edp auditors in progressive organizations are using computers in their work, including the use of a large number of generalized audit retrieval packages to analyze files. Less frequently used is test decking—running made-up transactions through the system off-line to establish the validity of the procedures. Some auditors use the integrated test facility technique which is similar to test decking, but is done to the live system. In program simulation a small but sensitive portion of a major system is modeled in a high level language and results compared to the live system. Among other techniques are sampling the files on- or off-line: tagging input and "picture taking," which is the output of the status of the tagged transaction at various points in the processing; and the use of flowcharting, test data generator, and librarian packages. The trends in edp auditing are significant. In a recent large class on advanced audit techniques almost half of the auditors were former computer professionals. More and more edp auditors are participating in system development projects as control specialist consultants and reviewers. Some managements are requiring an audit review of sensitive new systems as a standard procedure.

DISASTER PLANS AND SIMULATIONS

It takes considerable time, money, and knowledge to develop a good computer disaster plan. (One company spent a full man-year of data processing staff time studying the recovery planning for only key cash-flow applications on the computer.) It helps to involve the many people outside data processing who can contribute and an attempt should be made to quantify risks and costs even if the numbers are very rough.

The few organizations that have conducted computer disaster simulations have almost always been appalled by the results. Typically, records could not be reconstructed, backup didn't work as planned, costs would be considerably in excess of insurance coverage, and so on. There are two basic approaches to the problem. The first involves a series of mock disasters of increasing severity; this gradually exposes vulnerabilities and deficiencies. The second is to have one large-scale, full-blown simulated disaster. As deficiencies are uncovered, they are corrected and the exercise is permitted to continue. The time and money invested in such simulations is very worthwhile according to the organizations who have tried them.

CONCLUSIONS

This overview of computer security has stressed the heavy responsibility of data processing management. But computer security is too great a hazard to be the exclusive concern of an often harried data processing staff. Hence, top management, auditors, security and insurance specialists, key users and others must be involved. You must as-

sume that a disaster will inevitably afflict the computer function in your organization. The only question is when. How well prepared are you for this eventuality?

The problem should not be avoided because of prior assumptions of high cost solutions. Many of the steps that can be taken to reduce risk significantly are, in fact, low cost ones. The tendency is to want to rely on hardware, elaborate approaches, and to worry about the more improbable risks. A better procedure is sufficient attention to computer security by all levels of management, high morale on the part of a computer staff that is well-trained and alert to the problems, good procedures and internal control, regular security audits, and plain common sense. Modest investments for computer security are also wise.

In particular, the newer, more complex, and more hazard-prone systems under development today require more and better security planning at an earlier stage in the system cycle. The systems staff will need help in this activity from the hardware and software vendors, internal and external auditors, and consultants. We must have proper respect for the security challenges which such systems pose.

Computer security should rank high in a data processing manager's job description. It also merits a good deal of his time. The job (and company) he saves thereby may well be his own. The philosophy must be "It can happen here, but it must not!"

Mr. Weiss has worked in the dp industry since 1952, and at one time was in charge of all customer support for GE computers. He is a CPA, a Certified Internal Auditor, and has the DPMA CDP certificate. As director of the Automation Training Center, he conducts all computer-related training for The Institute of Internal Auditors and holds seminars on computer security for the American Institute of Certified Public Accountants. He is also the publisher of "EDPACS," The EDP Audit, Control and Security Newsletter.

[From *Datamation*, January 1974]

SOFTWARE SECURITY

(By Jacob Palme)

The safe operation of a computer can be disturbed either by unintentional errors or by intentional interference. Many protective measures guard against both intentional and unintentional damage—the backing-up of valuable data for example. This tutorial is, however, mainly oriented toward protection against intentional damage.

The basic methods of protecting any valuable property also apply to a computer: locks, alarms, personnel control, etc. This article will not discuss such methods. It will present those protective measures particular to computers.

The damage can be divided into three categories:

1. illegal access to data,
2. illegal modification, addition or destruction of data, and
3. interference with the ordered working of the computer.

This tutorial presents many different security measures aimed at protecting against different types of illegal penetration. The reader

should not be misled by this into believing that a safe system can be created by applying only selected protective measures against those penetration risks which are most acute, for this is very seldom true. If there is one unprotected module in a computer, then this module can often be used to circumvent the protection of other modules. Thus, full security usually requires that all modules are protected by a series of different protective measures.

IDENTIFICATION

Before a user is allowed to use a computer, he must identify himself to the system. This identification is usually done using some kind of key (or code). The key can be personal for each individual but sometimes groups of people using the computer for similar applications will have a single key in common.

Personal keys are safer than group keys because they are easier to change if there is a risk that some unauthorized person has possession of a key. With personal keys, people can be moved out of a group using the same data without changing the key for the whole group. Also, if something suspicious happens, the individuals who were using the computer at the time can be identified.

At individual terminals this identification is usually done by punching in an alphanumeric key on the keyboard. Here are some rules for choosing a safe key :

1. The number of combinations must be so large that there is little risk that someone hits on a legal key by chance.
2. The key should be selected randomly among all combinations. A user should not be permitted to choose the key himself. A better practice is to have someone responsible for distributing the keys when needed.
3. The key should be easy to memorize. The risk of unauthorized use is larger if it has to be written down.

A good compromise solution among these requirements is to have a key consisting of three random letters followed by three random digits. It is important that the computer never outputs the keys anywhere. Especially, they should not be readable at the terminal when they are put in.

It is also important that an alarm is given as soon as a terminal has made two or three attempts at entering an illegal key. Each such alarm must also lead to an investigation into what happened.

An alternative to a memorized key is to have some kind of reading device on the terminal, which can read the key from a punched card, a magnetized slip or an identity card.

The disadvantage of this is that the key will now be a physical object which can fall into unauthorized hands. The advantages are that no one can get the key by watching the hands of another person when he punches in his memorized key, and it is convenient for people who have to enter it frequently.

Both of these identification methods can also be combined, with one key read from an identity card combined with another key input through the terminal keyboard.

An additional security measure would be to identify not only the user, but also the terminal. If the terminal uses a dial-up line, this

identification can be done by a module in the terminal sending a terminal identification key to the computer.

An alternative to the use of keys is for the user to give his name to the computer without coding. Some kind of watchman will then have to check that the name and the user correspond. This is common for batch processing. Both the leaving and fetching of data must be checked manually.

In some cases, a person can have a terminal exclusively, locked when not in use; then no identification may be necessary.

It is important that you should be able to choose keywords (passwords) freely, and be able to change each one independently of all others. In some systems, the keyword is created by some secret transformation on the user name, the user number or other nonsecret information. In this way, those systems save the space of a keyword table. But such systems are not as secure. Keyword tables are not very big, and give much better security.

AUTHORIZATION

When a user has proved his identity to the computer, the computer can determine to what data and what programs he can have access. The user can be prevented from reaching data other than that for which he has need and the authority for use.

Authorization is done by some kind of table in the computer. The most general way is if every group of data is associated with a list of those people who are permitted to use the data in the group.

An alternative method is to put all people and all groups of data into a hierarchial (tree-structured) organization graph. A person is then only allowed to use the data which is in his own part of the organizational tree. Data near the root of the tree will thus be more generally accessible than data closer to the leaves.

The advantage of such a tree graph is that the storage requirement and the search time for the authorization tables will be lower. The disadvantage is that a group of data cannot be shared by two users without making it accessible to all the people in the smallest subtree containing the two users.

The authorization should not be strictly access or no access. Full flexibility requires that a person is given different privileges for different kinds of access:

The right to read a group of data.

The right to add to a group of data.

The right to change existing data.

The right to delete from a group of data.

The right to execute a program.

The right to change a program.

In the text above, I have intentionally used the term "group of data" and not "file." From a security viewpoint, a person may be allowed access to, for example, only certain fields in each record, or only some of the records in a file.

Usually, the operating system of the computer takes care of the authorization for whole files. Authorization which requires a file to be divided into different parts available to different users is usually done by user programs, not by the operating system. Such user pro-

grams must be execute only, so that the user cannot look at or tamper with the program. Also, the access to a certain file must be restricted to a certain user program, so that users cannot bypass the security checks in the special user program.

In advanced, relational data bases, the division of the data into secret and open categories, is very difficult, because data can be deduced from other data. For example, a user knows that there is only one 22-year-old mother with five children in a village. He wants to find her income, which is secret. The system can easily stop him from asking directly, "What is the mean income of all 22-year-old mothers of five?" The system does not answer such a question for groups smaller than say, a hundred people. But the user can instead ask, "What is the number and mean income of 22-30-year-old mothers of five, and of 23-30-year-old mothers of five?" If both of these groups are larger than a hundred people, he gets his answer and can deduce the secret fact from the open facts.

One way to protect against this might be that the computer remembers all previous questions. Each new question would then be related to the set of all previous questions, to see if the user can deduce protected information by combining answers. In practice, this would probably be impossible, especially since two users could collaborate to cheat the system, by asking one question each so that the protected information could be deduced from a combination of the two answers.

Another solution is to introduce artificial random errors into the answers given by the computer. These errors will be small for statistics based on large groups, but will be large for statistics based on small groups and very large on statistics based on only one individual.

Suppose, for example, that a user asks the system for the sum of the incomes in a group of 500 persons, and also for the sum of the incomes in a subgroup of 499 persons. If the sums were exact, then he could deduct the income of the 500th person by just subtracting the two sums. But suppose that the system enters a random error of about 1 percent in both sums. One percent of the sum of 500 incomes will be five mean incomes. The error in the difference will thus be between seven and ten mean incomes (depending on what kind of error you are talking about). And an error of seven or ten mean incomes will usually remove all information from the income of a single person.

The user could cheat such a system by asking the same question more than once and computing the mean of the answers; that way he could lower the error. Therefore, the same question always ought to get the same random error into the answer. This can be achieved by computing a pseudo-random error based on a hashing of the true facts which are hidden.

A well-known variation of this is to enter errors into the facts before they are stored in the computer. Therefore, you can never know whether an individual item in the computer is true or not. But if you compute a sum or an average on a large group, then the errors in the facts will tend to cancel each other, so that the relative error variance in a sum from a large group is much smaller than the relative error in each single factual item.

This is sometimes done in statistical surveys when people are asked questions which they do not want to answer. Instead of asking each

woman, "Have you had an abortion?" which she might not like to answer, she is asked to throw a die in such a way that only she knows the figure. She is then told, "Answer yes if either you have had an abortion or the die showed a six." Since only she knows the figure of the die, her secret is kept. The computer or the statistician will never be able to tell that she personally has had an abortion. But the error introduced by the die will, except for a small error variance, be removable from the mean of a large population.

The statistical methods described above cannot, of course, be used to protect all kinds of data. But the statistical situation is a very common one: A person planning where to set up a new petrol station or a new day nursery needs facts about the number of cars or the number of working mothers in an area, but he does not need to know the facts for a certain single individual. These facts are the ones we most want to protect.

FILE KEYWORDS, TRANSFER, CHECKING

An alternative to the combination of identification and authorization described above is to have keys connected not to individual people, but to files. Everyone who knows the key is allowed access to the file.

The advantage of this is that the group of people who are allowed access to each file can vary without restraint. But there are also great disadvantages:

The number of times a keyword is handled will be much larger, creating a greater risk that the keyword comes into illegal hands.

A person has to use not just one, but many keys. He cannot learn them all by heart, so he must use a list of keys, which someone else might see.

Keywords known to many people are also more difficult to change than individual keys.

Some very advanced systems also contain protection against transferring data from a file accessible to few people to a file accessible to many people. Therefore, even a person who has access to both files is not allowed to make the transfer.

An important part of the regular security measures must be continuous monitoring and logging of what is happening in the computer. This information can be consulted afterwards if something irregular has happened. The security monitor can also give an alarm if something unusual happens or when someone makes an unsuccessful attempt at illegal data access.

Very important it is that these monitor alarms are *really* checked by a human security supervisor . . . and that checking must occur immediately upon the alarm signal.

One method of protection against illegal introduction of data into a computer is to have some kind of redundancy in the data base. The same fact is stored more than once, and the correspondence between different data items is checked regularly.

PREVENTING ILLEGAL PENETRATION

All electronic equipment at a computer and its terminals emits electromagnetic radiation. Although this radiation contains informa-

tion which is handled by the computer, a spy close to a computer will get so many different signals mixed together, that he will find it very difficult to get anything out of them.

The more freedom and flexibility you want to give to the users of a computer, the more difficult you will find it to stop illegal penetration. The smallest risk will, therefore, occur for those users who are only allowed to communicate with one special user program. This user program can then check all messages from the user. This control is easier if the user can only transmit a small number of different kinds of messages, but, of course, this is not flexible for the user.

It is very important that such a user is never permitted to communicate with anything but that special user program. In some systems, a terminal can disassociate itself from a user program by means of special interrupt signals to the operating system. Such signals should not be permitted if they are not indispensable.

The most sensitive parts of a computer are I/O units like typewriter terminals and line printers, because here secret information in a readable form is transmitted rather slowly. By surrounding all such I/O units by a 300-foot fenced-off area, the risk of the normal radiation from the computer is small.

If, however, a spy succeeds in placing an electronic bug with a wireless transmitter into the computer with a circuit card, the risk is much higher. Such bugs can be detected in the same way as are voice-transmitting bugs.

A computer can be protected by shielding, if this shielding is done carefully. The shielding should be done with steel plates (not too thin). Rigorous requirements must be put on the tightness of joints, and doors and windows must be kept closed. Electrical and telephone lines into the shielded area must be filtered and water pipes protected.

The worst exposure stems from electronic penetration on lines to distant terminals. An important way of protecting such lines is cryptography. Cryptography security is good only if the end points of the line are well protected by other means. This will be discussed in more detail later on.

There are more ways for programmers to circumvent protective measures. In most computer systems, the intention of the operating system is to let programmers have access to almost all the resources of the computer when needed. To do this, and at the same time to stop illegal penetration by the same programmers, advanced and sophisticated security measures in the software are necessary. An alternative to this is to limit the resources available to a programmer. This is especially important when many programmers together are producing a large system, and you want to stop one of them from entering a private modification to suit his own personal needs (e.g., transferring money to his own account or logging confidential information on his own personal file). To safeguard against this, the manager of the software project must check that each programmer writes modules that stay within their prescribed bounds—modules which only access programs and data outside the module in permitted ways. You can get help from the computer in doing this if you only permit the programmers to use one special programming system which has a very secure compiler and run-time system. A secure compiler and run-time

system means one which checks the user program against all language errors, both at compile time and, if necessary, at execution time. A simple example is arrays. If the programming language system does not stop a programmer from exceeding the dimensions of an array, then he can illegally access or modify any word in his program, in other modules of the program (written by other programmers) and (on some computers) in the operating system of the computer.

A secure compiler should also make sure that separate modules of a large program can only interface in certain permitted ways. That way, the modules can check on each other; e.g., one module can check the legality of instructions which one module gets from another one.

In the future, computers will probably have larger virtual memories, and so the protection provided by a compiler within the memory will be more and more important.

Programming language systems today are seldom very secure. Sometimes there are protective checks such as those to prohibit exceeding array bounds. But often, the programmer is allowed to set a switch which disconnects these checks.

Compilers which allow separately compiled modules are very seldom secure. The reason for this is that they usually do not compare two separately compiled modules to find inconsistencies. For example, FORTRAN compilers seldom check the consistency of COMMON blocks. However, a compiler with separately compiled modules can be made secure.

Another common way of gaining security by restricting the freedom of the user is to disallow the usage of certain central utility programs for file handling. However, if the system is not protected against this, a penetrator might take such a utility program from another installation. The method of maintaining security by restricting the programmer's freedom is therefore not usually very effective.

The group of people who have the greatest need to access all the resources of the computer are the systems programmers. Therefore, there is usually no possibility of protecting a computer against illegal penetration by a systems programmer or an advanced operator.

RESOURCES TO BE PROTECTED

If you want to stop the advanced programmer from circumventing the security measures, then all resources available to the programmer must be protected. Important resources are primary memory, processor, utility programs, and external memories.

The protective measures in the hardware divide the primary memory into different sections, one for each user program. A mechanism in the hardware stops a user program from reaching primary memory outside his own area. This mechanism should protect separately against writing, reading, and execution.

Note that the operating system is also a program. Even computers which are not multiprogrammed (where only one user program at a time is present in the primary memory) must have some kind of hardware protection of the primary memory. A program which can get at the operating system can thereby have access to everything else in the computer system.

Sometimes there is a need for two programs to communicate or use common data. In the simplest case, a user program must communicate with the operating system. This communication can be arranged in such a way that the operating system is always "master" and the user program "slave." The user program can ask the operating system to do certain things or to deliver certain data. But the operating system should always make a full check of the correctness and legality of the user program's request before the task is performed.

Two user programs may wish to share a common data area. Usually, this common area is write-protected for both programs as in a "re-entrant" program; in such cases, a user program can read and execute both his own memory area and the common area, but cannot write in the common area. The program in the common area can access the memory of both user programs, but usually cannot write in the common area.

The program in the common memory area should not, of course, have access to anything but those user programs which share this common program. In some computers, such a common program has access to the whole memory; in this case the program must be very carefully checked, or such common programs cannot be used.

The central processor in most computers is allowed to govern everything that is happening in the computer. A secure system, therefore, cannot give the programmer direct access to all resources of the cpu. Usually, the cpu's resources are divided into two groups: common and privileged operations. The common operations are available to all programs; the privileged are only available to the operating system. Another, similar, solution would be to have a separate cpu for the privileged operations.

If a user program wishes to perform a privileged operation, this must be done indirectly. The user program sends a message to the operating system, which first checks the admissibility of the message, and then performs it.

All transmission of data between different memory units and to and from peripheral units are privileged operations. All changes in the security system of a computer, like changes in the memory protection, are also privileged.

The operating system is usually protected against access from a user program, and many central operations which are especially dangerous may only be performed by the operating system.

Security checks in the software should be in the operating system, not in user programs, if possible. The reasons for this are:

1. The operating system is usually the most thoroughly checked program, and security measures, especially, must be thoroughly checked.
2. The operating system is common to all users at the computer. Protective measures in the operating system will therefore give an even, high quality of the security for everything done on the computer.
3. The operating system is often very difficult for a manipulating programmer to access.

To illustrate some of these points: the central memory areas of a user program should be zeroed when the user program releases them, otherwise another user program might get data from a previous program using the same memory areas. This zeroing can be done either by

the operating system or by the user program. However, check the arguments again in these special cases:

1. If a user program aborts because of an execution error, then often the final parts of the program are never executed. Thus, the zeroing of memory may not be done. If, however, the zeroing is done by the operating system, then it is always done, regardless of what happened in the user program.
2. All programs always get their memory zeroed after use, if this zeroing is done by the operating system.
3. An illegally manipulating programmer would find it more difficult to remove the zeroing routine from the operating system than from a user program.

WEAK POINTS IN THE OPERATING SYSTEM

Even if the operating system is one of the best-tested and protected programs in a computer, some mistakes cannot be avoided. Some of these may perhaps be used to advantage by a skilled penetrator. Every such error is unique and difficult to classify, but there are examples of often occurring weak points in operating systems.

1. When a user program asks the operating system to do something, the legality of the requirement is not always fully checked.
2. The user program succeeds in changing its message to the operating system after it has been checked by the operating system, but before it has been performed.
3. The operating system stores information in the user memory area (e.g., I/O buffers with associated information) and the user program succeeds in changing this information so that it will be misinterpreted later on by the operating system.
4. There is an intentional opening in the operating system which was put in to help system programmers or to help advanced utility programs. But this opening can be misused by other programs. This opening might also have been introduced intentionally for later use by a spy in the group writing the operating system.

Two common reasons for such weak points in the operating system are that the cost for full security is regarded as too large, or that the operating system is so large and complex that no one understands all the types of interaction that can occur inside it.

An operating system can be written so that the risk of such weak points is lessened. It can be divided into many subprograms which are all protected from each other as well as if they had been user programs. When one of these subprograms asks another to perform a task for it, the request is checked in the same way as requests from user programs are checked. This kind of operating system design has many security advantages: a penetrator which gets into one "room" does not immediately get into all the other "rooms"; the most dangerous operations can be confined in "rooms" many doors away from the user programs; each subprogram can be checked more carefully than the whole operating system.

For a user who already has an operating system, these design principles are not of much value. He can, however, gain higher security by using an older, better-tested version of the system, and he can also "mine" the operating system. "Mining" is a method of protection

against a skilled penetrator who has detailed knowledge of the operating system acquired at another installation. By putting in special security checks and by changing some important data fields, the penetrator is lured into betraying himself. A successful penetrator must succeed in doing what he wants without anyone discovering what has happened. But the operating system is usually so vulnerable that a penetrator can easily cause a system crash, especially if some things are not quite what he expected. An analysis of the system crash can show what had happened.

You can feel more sure of the security in a small operating system than in a large one. Some computers move as many operating system tasks as possible into user programs so that the central, sensitive part of the system becomes smaller. This gives better security, but only if these special user programs themselves (sometimes called utility programs or cusps) are fully protected from the user. Very valuable is a system where a program can be executed in the user area, but where the user has no other access to it than the execution right (not even the right to read or dump the concealed program area). This means that the hardware memory check must differentiate between the right to write, the right to read, and the right to execute in a certain memory area.

Some central user programs have a position in-between the operating system and the ordinary user programs. Examples are compilers, interpreters and file handling systems. These programs must be protected against illegal access. The ordinary user should be able to execute them only, but not do anything else with them.

To keep the central operating system small, it must also be protected against these central user programs, just as if they were ordinary user programs.

Access to external memories is usually through a central file handling system which is part of the operating system. The protective measures are described above under the heading "Authorization."

It is very important that the system always zero all files as soon as they are released by a user. This should also be done for temporary files and for primary or virtual memory.

Zeroing does not give full security for such volumes as tapes and removable disc packs which can be taken from the computer. Special treatment can divulge information even after several over-writings with random noise.

CRYPTOGRAPHY

Cryptography is a transformation of data which makes it unreadable to a person who does not have access to the cryptographic key. The transformation can be done by either hardware or software.

One transformation which cannot be broken is to use as key a genuine random number (not a so-called pseudo-random number) which is as long as the data to be transmitted. Two copies are kept of the key: one at the transmitter, one at the receiver. The sender adds the key to the message (addition without carry is usually best) and the receiver subtracts the key to get back the message. When the key has been used once, it is consumed and cannot be used again.

If the sender and the receiver are both safe, this gives full protection to the communications line. But do not forget: a) If someone gets

hold of the key, he can also decipher the message. The keys must therefore be treated as secret both before and after use. The keys themselves cannot be transmitted through the communications line. b) This kind of cryptography gives only protection of the communications line. At the sending and receiving ends, the message is used uncoded. For example, you must ensure that no one is able to modify the cryptographic equipment itself in such a way that the message can be understood by someone listening in on the communications line.

These observations mean that you can very seldom make an information system safe by introducing cryptography. Cryptography is of value only if there is a single known weak point in an otherwise safe system. But the cryptographic routines themselves, and all parts of the system where uncoded data is processed, must be fully protected by means other than cryptography. And if these other means are good, then cryptography may not be needed at all.

The cryptographic method described above requires a key as large as the amount of data to be protected. This is often not practical; a shorter key can be made to generate a longer series of numbers.

Although very often a person who is not an expert believes that he has found a safe cryptographic method, these tasks should not be given to amateurs.

Practical requirements of a cryptographic method :

1. Some cryptographic methods require that a large file be ciphered and deciphered in sequence from the beginning of the file. But for direct access application, you need a method which can directly cipher or decipher any randomly selected record in the file.

2. If an error comes into the transmitted signal, then only a small part should be lost, not the whole remainder of the message.

A way of moving the security problem away from the computer is to have computers wholly dedicated to a secret task (at least for certain shifts) so that input and output goes only to those who are allowed access to the secret information. This is the only method allowed for highly secret military data in most countries. This method is very expensive for large computers, but is less costly if the task can be done on a minicomputer.

If there is one weak point in a security system, then very often that weak point can be used by a skilled person to penetrate all the other parts.

Say, for example, that a system has good protection of data, but not full protection of user programs. A penetrator can then modify the used programs, so that they will later on divulge the secret data.

The central point of security on a computer is the operating system and the basic hardware. No gadgetry like cryptography or errors intentionally introduced into the data will give security if there are loopholes in the operating system or the central hardware. In my opinion, too much is said about such special methods, and too little about the central security measures. These special methods are sometimes very interesting, clever, and valuable, but when a manufacturer talks too much about them, this may be a smoke-screen to hide more basic insecurities of his system.

Mr. Palme is head of the datalogy (non-numerical computer science) section of the Research Institute of National Defense, Stock-

holm. He has been working with simulation models, with development of the SIMULA 67 programming language, and with computer systems understanding natural human languages. He has also written several crime novels.

[From Electronics, July 25, 1974]

U.S. TO REQUIRE COMPUTER SECURITY

(By Larry Marion, Washington Bureau)

Computer privacy is coming, but it isn't going to come cheap. That's the message for hardware makers in bills that are starting to make their way through the Federal legislative process. When these measures, seeking better security for government data banks, are boiled down into a law—and experts expect one this year—security devices for Federal, state, and local government data banks containing personal information will be mandatory. Senate committee statistics indicate that there are dozens of Federal installations alone and hundreds more at other levels of government.

Access controls, including substantial record-keeping systems, would require installation of costly security systems. Ruth M. Davis, director of the National Bureau of Standards Institute for Computer Science and Technology, says the majority of the privacy requirements would be met by "hardware implementation."

Computer security has been a major concern for the last few years as hundreds of cases of computer manipulation for personal profit have been uncovered. Banks, telephone companies, and retail outlets have investigated various methods of limiting access to files containing information, such as accounts receivable and cash deposit totals. Time-sharing centers have been especially interested in preventing fraudulent billing schemes.

DEVELOPMENT NEEDED

Experts in industry and government expect access controls to be offered by computer vendors within the next three of four years, but Davis and another expert, Rand Corp. analyst Willis Ware, say that these systems are not now available on the commercial market. Davis says that techniques and systems developed for the military could be adapted by commercial firms "when the incentive is there." Such techniques—including voiceprints, fingerprints, hand geometry and magnetic cards—can be circumvented or have not been sufficiently developed, Davis has told a Senate committee. Experts say the cost of secure-access devices, between \$20,000 and \$30,000 per four-terminal data bank, may be too high.

Davis sees security as "a whole new market for the future. No one has gotten beyond the superficial level of computer-security devices. At this time, we don't have the slightest idea what the total cost of security will be, but preliminary studies indicate the cost to the Federal Government would be between \$750,000 and \$5 million at the upper end of the spectrum, plus up to \$1 million per year in operating costs, depending on which legislation is passed. Encryption techniques

[guidelines on encryption are soon to be issued] will result in a four-fold increase in transmission.”

Rapid application of current technology, plus development of new technology, will be needed to meet the demands of the proposed legislation, she notes. And increased transmission lines and facilities would be needed to handle the extra load.

BILLS

Despite the warnings about cost and technology, there's no shortage of bills in the congressional hopper. The legislation includes formation of a Federal privacy board, to be responsible for annual reports on the size and number of Government data banks with personal information. Other proposals that are included in many of the more than 100 computer privacy proposals include requirements for recording each access to a system and keeping that information for two years or more.

Davis, at hearings of the Senate's constitutional rights subcommittee of the Judiciary Committee and the Senate Government Operations Committee, warned that such a requirement for information accessed only once in nine months would double a file's contents in seven years. Davis also noted that merely recording each access by the operator's name is not too difficult, but if the legislation requires a catalogue of facts—such as which part of the data bank was accessed, and what was reviewed and for how long—the resulting need for memory and operating costs would be exorbitant. She indicates that costs of increased memory capacity and the development and sale of access-control systems would have a major impact on the computer industry.

“Either a computer data bank has access controls or lots of insurance—those are the only two options I see in response to the security-privacy legislation now before Congress,” says Rand's Ware, who is also a technical consultant to Wema. He warns that it will be more difficult to apply access control to some computers than to others. For the data-bank operator, Ware says the new legislation would mean that more memory capacity would be devoted to housekeeping.

PACKAGES COMING

As for the vendor hardware, Ware says, “In the next three years, most hardware manufacturers will offer hardware-software security packages as part of a security safeguards system. And right now, there are not many gadgets around that can authenticate if the user is who he says he is.” Most of the proposed bills permit aggrieved citizens to sue computer data-bank owners if the owner/operator does not comply with privacy guarantees in the legislation, including prohibitions against improper disclosure of personal information.

The final Senate committee proposal should be before the floor for a vote by the end of the summer, according to Congressional staffers. They expect House action before Christmas. A computer-privacy bill is inevitable this year, they say, because it is a “computer-privacy-conscious” Congress. Sen. Sam Ervin (D, N.C.) a prime sponsor and mover of the computer-privacy legislation, makes the same prediction.

IMPACT

Already the specter of legislation has had an enormous impact. General Services Administrator Arthur F. Sampson has announced a new policy of submitting computer-procurement proposals to Congress before requesting bids, and the GSA now reviews the security requirements and features of in-house computer proposals from other executive agencies [*Electronics*, June 27, p. 30]. Proposed major system purchases for the Internal Revenue Service, the Veterans Administration, and the Justice Department are being held.

The GSA delay in future computer and telecommunications procurements stems from the recent furor among the agency, Congress, and the White House Office of Telecommunications Policy over a large computer-procurement proposal issued in February but withdrawn in May. GSA wanted to purchase up to 10 large computer centers for it and the Agriculture Department—all connected by a dedicated network. OTP objected to the size of the purchase, the failure of GSA to try for leased telecommunications systems, and the absence of detailed cost estimates for the package.

GSA will issue an amended request for proposals this summer for a smaller computer system without a telecommunications network. The agency temporarily will use its Federal telecommunications system but issue an RFP on a telecommunications network next year unless Congress intervenes.

SWEDEN'S WATCHDOG

Sweden's Data Inspectorate—the world's first data-bank watchdog—has made its first major decisions. The rulings are expected to have long-range effect on private data banks in that country. Perhaps the most important is rejection of a plan by the nation's banks to establish a national repository of information on all Swedes to be used for credit and other financial transactions. Each bank will be permitted to operate data banks only on its own customers.

The Swedish privacy laws and those being submitted to the U.S. Congress have basic differences. The American versions are concerned to a major extent with computer security, as well as privacy. On the other hand, the year-old Swedish law [*Electronics*, July 19, 1973, p. 72] prevents, among other things, keeping records of highly personal matters, gives each citizen the right to get a free printout of his "dossier," forces data banks to correct errors or eliminate names on request, and gives citizens the right to sue data banks.

[From the Magazine of Bank Administration, October 1974]

HOW TO IDENTIFY COMPUTER VULNERABILITY

(By Lindsay L. Baird, Jr.)

The computer is a vital tool in the daily operations of both government and industry. As with all tools, man has found ways of utilizing the computer to achieve unlawful personal gains. It has only been within the past decade that the problem of computer assisted or related crimes has surfaced. In most instances, these crimes have impacted on the efficiency and economic well being of industry.

Computer security has become a topic that is frequently discussed in the board rooms of industry. In the recent past, computer security was

often discussed, but viewed as something no one could really do anything about. This attitude is changing, as management concern grows about the security of vital data received, processed, stored or transmitted by data processing systems.

Let us briefly review first how various individuals in industry and government frequently view the subject of computer security. Security managers, as a professional group, have not acquired the detailed knowledge required to adequately address all the security problems associated with computing systems. They experience no problem addressing physical security, personnel identification, access control and other related nontechnical functions. However, when the security staff is asked to address a hardware or software security feature, they are often bewildered by the electronic marvel confronting them. Confronted with this situation, the tendency is to throw up one's hands, lock everything up, mark all media as sensitive and require the system be operated in a dedicated mode.

Corporate management-executives are experiencing the same basic problems that have confronted security managers. They too have been intimidated by the mystique of the computer and its bits, bytes, flags and fields.

Data processing managers, on the other hand, have had a tendency to view security as a problem not requiring a great deal of concern and effort. They have a natural tendency to resist the requirements imposed by the security officer, viewing them as hamstringing operations and impacting on equipment efficiency. The ADP (automatic data processing) community often cannot see why the security manager is concerned when he cannot fully express exactly what the security problem is or may be. Besides, the vast majority of the files processed in any given application do not contain sensitive data—so why all the concern?

When industry first started to automate its business applications it was common to go about the process of automation in somewhat of a piecemeal manner. The first application automated was payroll and once that was functioning properly the decision was then made to automate something else—for example, accounts receivable, accounts payable, sales, etc.—one application at a time. Each application was a self-contained unit. As additional applications were added, the need developed for audit checks between each application and the total system.

One must remember that in a manual application there were a number of check points where the flow of paperwork would halt if certain actions had not been accomplished. It might be that a Mrs. Jones in the accounting department would not approve a request for payment until she had physical possession of certain source documents that were properly completed by two or more different departments. This people-interaction in many instances was reduced when a particular application was automated. When an audit trail or checkpoint system is developed for two or more of these independent applications, the end result often reduces the number of people involved and relies on system-generated checks. Now instead of a clerk reviewing individual purchase orders or other documentation he is found with a printout that reflects some if not all required information, but he no longer controls the source documentation.

Several years ago, while in the U.S. Army, I concluded that we were addressing our ADP security problems in the wrong manner. We were output oriented then, and today we continue down that path. We were looking at reams of printed matter and applying security markings because somewhere therein a secret might be found. Just what line or lines of output were sensitive was exceedingly hard to determine.

Frequently, while reviewing voluminous sensitive reports, I asked which particular lines or pages contained the information requiring protection. The results of these inquiries were quite informative. ADP personnel in almost all instances did not have the faintest idea what was sensitive. Security officers had some idea but they were more often in error when asked to be specific. It was functional personnel that were best at identifying specific lines of printout or pages that contained sensitive information, though they were often wrong also. It is obvious that something is wrong when we are unable to identify the information that requires protection.

I am certain that we all know what security is and what it means, but do we really know what we are developing or employing protection against? Have we defined, identified and isolated the specific threats to our computer systems? The answer to this question in most instances is an unqualified no. It is logical that the threats to and vulnerability of a computer facility or system must be determined before appropriate safeguards and counter measures can be developed and then employed.

Computer security is not a one man task as no one human being has the multitude of technical and functional skills required to properly address the problem. The skills required include, but are not limited to, the following: Systems analysis, programming, hardware, security, auditing, finance, communications, operations, supply or inventory, marketing, personnel, research and development, engineering and, above all, management.

COMPUTER SECURITY GROUP

The formation of a computer security group may be the most cost effective method of assessing the internal and external vulnerability of computing systems/facilities. This group should be headed by a senior member of management that has decision-making authority to resolve conflict on the spot. Full-time members would, as a minimum, include the security officer, internal auditor and the best systems analyst and programmer from the ADP department. Each functional area, such as accounting, personnel, operations, marketing, etc., would provide appropriate representation as required. The tasks of this computer security group would be threefold:

Develop secure automatic data processing facilities and systems that will dependably prevent deliberate or inadvertent access to material by unauthorized use of computers, associated peripheral devices, systems and data.

Develop standards and procedures for the analysis, design, testing and evaluation of the security features for the computing systems.

Develop procedures for the physical protection of automatic data processing facilities, systems and data.

To achieve these goals, the computer security group must conduct an indepth analysis and evaluation of their company's asset value, data criticality, system security, threat level and vulnerability.

ASSET VALUE

Most comptrollers and ADP managers can quote the dollar value their organizations have invested in facilities, computers, media and peripheral devices. However, quotations become hazy when one tries to determine capital investment in data base development, programs and documentation for major applications.

The first step in developing a computer security program is to determine the value of the assets requiring protection and the degree to which they are covered by insurance. This is best accomplished by listing each piece of equipment, its cost, replacement value and then determining the amount of replacement costs that insurance provides. Not all insurance policies are all-inclusive, and many have restrictive clauses that require a firm to perform certain functions or provide specific protective features if a claim is to be honored. A detailed review and evaluation by the insurance, safety, security and ADP departments will often discover non-compliance with insurance requirements and a potential for significant financial loss.

A second step is to determine which pieces of equipment are absolutely essential to daily operations of the data center. Once identified, the availability of replacement equipment must be determined. Can your firm wait three to six months for a replacement main frame? If not, have they developed an alternate source of required computing power and peripheral devices? In answering these and other obvious questions, the computer security group will be in a better position to evaluate and determine the cost implications of the unavailability of facilities, computers and peripheral equipment.

Hardware can be replaced with relative ease; however, the loss or destruction of the data base or application programs and documentation can be catastrophic. The cost and effort devoted to data base development and application documentation are significant and frequently exceed the value of the hardware several times over. It is not a simple task to determine direct costs, replacement cost and financial loss a firm may suffer if these vital assets are lost or destroyed. Yet it is important to conduct such an analysis and then equate the adequacy of insurance coverage.

We now have an integrated data base that many functional areas share. Frequently computer-generated output contains information that was placed into the data base by two or more functional areas. An example can illustrate the point.

World-wide assets of many ammunition end items are classified at the "Secret" level. The cataloguing activity typically inputs to the data base federal stock number, DOD ammunition code, narrative description of the end item and unit price (each data element standing alone or in combination are unclassified). The supply activities unclassified input may include storage location, condition code and quantities (quantities at one or more storage locations, but not all, are unclassified).

Let us now insert a third party—the Comptroller. He has a requirement to conduct a one-time dollar value analysis of selected items in the inventory. The data processing division is asked for help, which they willingly supply. The Comptroller asks for a report by end items with narrative description, storage location, value of the inventory at each location and, as a second thought, summary totals and unit prices are asked for “in order that his people can get some feel for the volume.” The results in this case—a Secret report which was composed of unclassified (while standing alone) data elements. Were we to go back to the originators of the basic data elements, they would rightfully state that they did not cause a security violation. The Comptroller could also state that his people were faultless—the inputs were unclassified and they were not aware that the combination would result in a classified output. The data processing people also claimed innocence as they were machine drivers that were processing two unclassified file segments. Where was the Security Officer? In his office, most likely, as no one had any indication that they were heading into troubled waters. Even had the Security Officer been called in for assistance, it is doubtful that he would have known that a security violation was in the offing. Let us now compound the problem a little further by hanging some remote terminals on a system. The buzz words “dial-up,” “real-time” and “management information” should send security shock waves up and down the spines of man. If you are currently unable to identify which line(s) of data within a printout or what combinations of data elements or file segments are classified, then you have another major security problem. An example using world-wide asset data again: A remote terminal could perhaps legitimately inquire as to what storage facilities had a particular item in stock. Once a list of storage locations was generated, the terminal operator could request the quantities on hand—location by location. Each individual response is unclassified; however, the sum of the individual totals is classified at the Secret level.

Let us assume that our remote terminals are in secure areas and all operators are properly cleared. Unless all data transmitted is treated as classified information, the potential for a security violation will exist. There are very few computing systems and related software that either notify terminals that the content of data transmitted is classified or generate an audit log reflecting the creation of an accountable document at a particular terminal. It would be a gross error to rely on a terminal operator to determine what hard copy documentation required protection.

Government and defense industries are not the only ones that are confronted with these security problems. Substitute proprietary for secret, confidentiality or privacy for classified, marketing strategy for ammunition, etc., and it becomes obvious that industry has a significant problem.

How then are we to provide an acceptable level of protection for data resident in our computing systems? The first step is to require functional personnel to identify general categories of information that are critical to the operations of the organization. Governmental agencies would include such things as world-wide asset data or pre-procurement information as sensitive. Industry, on the other hand,

might include trade secrets or marketing data as information critical to their operation. Vital or critical data is best defined as: "That information which, were it disclosed to an unauthorized person or competitor, would cause embarrassment, benefit competitors, hinder contract negotiation, etc., or which, if lost, could lead to either financial loss or an adverse impact upon operations.

Next, each general category of critical data is examined in detail to determine what data elements or combinations of data elements will produce information requiring protection. This can be an exceedingly difficult and time-consuming task. It may be impractical from a cost effectiveness point of view to identify all combinations that produce vital data, depending on the size and complexity of the data base. However, the computer security group should take the time to at least partially go through this process in order to obtain some insight of the complexity combinations of data elements present.

An alternative to identifying combinations would be to review all reports and other documentation generated by the computer system. The task here is for a functional specialist to identify that vital information contained in these outputs, line by line or page by page. Determinations should also be made as to the degree of sensitivity, who has a "need-to-know" or a "need-to-access," the number of copies and the distribution requirements. Assuming that the reports and other documentation generated by the computing system satisfy the needs of management, then there should be no requirement for data to be displayed in any formats other than those already prescribed. Now, all output from the system via printers, CRTs and hard copy terminals, etc., can be restricted to prescribed formats and the problems of data base manipulation are reduced significantly. It is relatively easy to create a security matrix which can automatically identify lines or pages of output requiring protection, annotate the degree of sensitivity and initiate a system generated audit trail.

SYSTEM SECURITY

We must determine a computing system vulnerability before adequate safeguards can be designed and applied. A comprehensive review of current systems and applications that utilize vital data and files or produces sensitive reports is the next task for the computer security group. This review should evaluate the following:

Disaster prevention to include backup data and files, adequacy of program documentation, fallback equipment and established recovery procedures.

Safeguards to prevent accidental or malicious alteration or destruction of data.

Potential for unauthorized use of the system.

Potential for manipulation of systems and data to perpetuate fraud, embezzlement or other crimes.

Control of access to vital data, files and reports.

Operating controls.

Adequacy, appropriateness and enforcement of current security measures.

Safety programs and equipment.

Personnel security programs.

The best approach to determining software vulnerability is to select one or two applications for study. An excellent method of initiating this evaluation is to call in either the programmer/analyst that designed the application, or the individual responsible for program maintenance. Require him to present an overview of what the application is designed to perform and then ask him how many ways he can subvert the system. Odds are that he can rattle off a half dozen simple but effective modifications that would result in undetected losses.

Fortunately, most humans are honest. A detailed study of an application by a system analyst and programmer with the assistance of a functional specialist will invariably develop additional ways the system may be subverted. There are several schools of thought on what is needed to eliminate those "holes" in the system. One is that minor system design modification and program change will be sufficient. The other is that the entire system must be redesigned. I believe that patching holes is not adequate. In most instances, at the time the application had been designed, there was little if any thought given to security, and perhaps only moderate concern for auditability. Any application that processes vital data and assets must be designed from the very beginning with auditability and security in mind. This will become more evident as the computer security group continues its evaluation of additional applications. They will find a number of different applications have multiple interfaces with each other, and each of these may contain "holes." A patch may correct a deficiency in one application but may not be sufficient when that application interfaces with others. This will be especially evident in systems where applications were designed and implemented in a piecemeal manner.

Redesign and software development will obviously present itself as a logical approach to eliminating many security and auditability weak points; however, in most instances this will be exceedingly costly and management in all probability will not authorize the expenditure of funds. Knowing your vulnerability and correcting as many deficiencies as is practical may be the only available alternatives. This alone is a major step forward—for you are now able to define specific system security weakness. The old adage, "A problem well-defined is half solved," best points this out.

THREAT LEVEL

The computer security group's next task is to evaluate all previously assembled information and prepare a comprehensive analysis of actual and potential threats to the automatic data processing system and data base. This evaluation should provide an objective rating of the adequacy and effectiveness of existing security in the current system and facilities. It will identify security weaknesses and recommend corrective measures. Recommended remedial actions should be priority ranked in order of risk level and adverse impact should the potential or actual security hazard materialize. If at all possible, estimated or actual cost in manpower and funding should be developed for all recommended corrective measures.

VULNERABILITY

Never lose sight of the fact that there is no such thing as a totally secure automatic data processing system. Once security and audit weaknesses have been identified, and corrective measures developed and installed, a feeling of greater confidence will prevail.

The steps taken to provide a secure environment for the computer system only become a new challenge for the curious, dishonest or disgruntled employee. The computer security group should be given the responsibility of constantly testing and evaluating the security features of both the automatic data processing system itself and its external facilities. The technique should be to find if there are additional methods of penetrating the system and to attempt under controlled conditions thefts of material, vital information or dollars assets. A few areas that are deserving of such attention include: Administrative and security control procedures, operating systems, software (each major application), remote and report protection, and auditing.

CONCLUSION

The approach to achieving a more secure computer system environment as presented here is not an all inclusive solution to today's problems. It is a method of bringing together the multitude of talents required to properly define, identify and isolate the specific threats to computing systems. A systems analysis approach to identifying asset value, data criticality, systems security, threat level and vulnerability by a computer security group offers a cost effective method of assessing the integrity of computing systems and facilities.

Lindsay L. Baird, Jr., has more than 20 years' experience in law enforcement, industrial and physical security and contract administration, including 11 years in data processing and nine in intelligence and classification management.

[From the New York Times, Nov. 23, 1975]

LAW OFFICIALS WARN OF COMPUTER CRIME

Washington, Nov. 22 (AP)—Law enforcement officials have expressed concern about potential security problems if they should be required to share computers with other state and local agencies.

At a hearing on proposed regulations governing access to computerized criminal justice information systems, Adam D'Alessandro of New York State said Monday that shared systems could present "many potential threats" to the security of the law enforcement information.

He told the hearing, sponsored by the Law Enforcement Assistance Administration that while computer experts assure him that they can provide a system that is secure against penetration by unauthorized persons, such proposals "must be looked at with a jaundiced eye."

Mr. D'Alessandro acknowledged, however, that economic considerations would require that law enforcement officials share computer systems. In that case, he said, control over the entire system should remain with law enforcement officials.

A key issue in the proposed regulations is whether computers used for criminal justice information must be restricted to use by law enforcement agencies. As originally drafted the proposed regulations restricted the use, but an amended version would permit sharing computers with other government agencies.

Data Protection Through Cryptography



by Dennis K. Branstad*

COMPUTER networks may be the Federal paymasters of the future. Even today, computers typically process the payroll within each agency, print the checks at the Treasury Department, and credit the employees' accounts in local banks. However, several days often pass between these transactions.

If this information was electronically transmitted among computer facilities, it would arrive almost instantaneously. A vast number of automated functions could in fact be handled faster and more efficiently by "linking" independent computer facilities on a broader scale. However, over this technologically feasible vision of a vast computer

turn page

DATA *continued*

network hangs the spectre of accidental or intentional misuse. Consider, for example, the real possibility of an unscrupulous individual using electronic techniques to divert funds for personal advantage. This, of course, is a human problem. However, technology can provide the solution.

The National Bureau of Standards' Institute of Computer Sciences and Technology (ICST) is working on technology to protect data in computer systems. One effort to provide data protection through encryption technology is being carried out in the Systems and Software Division where a Federal standard is being prepared.

* Dr. Branstad is a Computer Security Project Leader within the NBS Systems and Software Division.



Computer cryptography is achieved through the use of an algorithm—a set of rules for accomplishing a specific task. An algorithm specifies the mathematical steps needed to encrypt the data. A number, called the "key," controls the encryption process. When data is encrypted, it is changed into an unintelligible form. The encrypted data can be decrypted—returned to its original, intelligible form—only by authorized receivers who have the same encryption key. The data is protected by keeping the key secret.

The processes of encryption and decryption can be used to protect the confidentiality of data because the data cannot be read without proper authorization. They can also be used to protect the integrity of data because any modification of the data in encrypted form becomes apparent when it is decrypted.

An electronic device can be constructed to perform the required steps of the encryption/decryption processes both reliably and efficiently. Modern technology makes it possible to perform many complex functions in a device incorporating a single electronic "chip." This technology makes possible the inexpensive and handy arithmetic calculators of today. The nearly 14,000 electronic logic elements needed to implement the data encryption algorithm may be contained in such a chip which is less than .635 centimeters (1/4 inch) on each side. The costs of producing this piece of electronic hardware may be as low as \$10 after the initial costs of production have been recovered.

An Algorithm

ICST sought an encryption algo-

ri thm for promulgation as a Federal Information Processing Standard (FIPS). This algorithm would have to provide a high degree of security, security based not on the secrecy of the algorithm itself but only on the secrecy of the key. The Institute solicited for suitable encryption algorithms and selected one submitted by the International Business Machines Corporation. This algorithm was published as a proposed standard on August 1, 1975, in the Federal Register.

Publication of the algorithm initiated the Federal standards-making process in this area. It is expected that adoption of the algorithm as a Federal standard will lead to voluntary adoption of the algorithm by computer users outside the Government. In fact, about 400 people from private organizations, both foreign and domestic, requested the algorithm after it was published for comment in the March 17, 1975, Federal Register. The size of the combined Federal and interested private sector market for a standard electronic encryption device should help bring the cost down.

First Users

When a Data Encryption Standard is established, it is expected to find many early uses such as protecting transactions conducted by the Federal Reserve System. These transactions often include the electronic transfer of vast amounts of money among the twelve Federal Reserve regions covering the United States.

In addition, the Federal Home Loan Bank Board has solicited for data encryption protection to be incorporated in its future procurements

of data processing equipment. The requirements that have been defined for this protection can be satisfied through the use of this data encryption algorithm.

Estimates of grain production and oil reserves have a significant effect on the commodity market or the stock market. Acquisition of this information as it is being electronically forwarded to Washington and before it is publicly released could give an individual an unfair advantage in reaping tremendous financial returns. Use of data encryption can prevent the possibility of such an event.

Other Uses

In addition to protecting transmitted computer data, devices implementing the Data Encryption Standard may be used to authenticate the holder of a banking or credit card. Information (the encryption key) known only by the authorized holder of a card may be used to decrypt information stored on the card and hence to gain access to modern, automated banking terminals or to prove the validity of a credit purchase of merchandise.

Access to a computer network having sensitive information may be granted or denied to an individual based on the individual having or knowing a proper encryption key. Control of access to computers and networks may be enforced by developing new technologies based on encryption techniques.

"Computer networks are emerging as a powerful national force touching every individual in Society" (*DIMENSIONS/NBS*, April 1975). NBS is providing a means for protecting data being transmitted within those networks. *continued on page 214*

The art of cryptography, or literally, "hidden writing," developed independently in a number of ancient civilizations, including Egypt, India, and Mesopotamia. By systematizing cryptographic techniques, the ancient Arabs became the first to transform this art into a science. The message concealed in the cryptogram expresses the relationship between cryptography and the computer.

RRFYM	ATGTC	RATFC	FAEEO	REERO
NPDPS	NORDT	SCTHA	TMPEE	NMNY
HOOTI	RICPO	USNST	TPEMC	AOOER

H.

If you need help in arriving at the solution, see page 214.

EXECUTIVE GUIDE TO COMPUTER SECURITY

(U.S. Department of Commerce, National Bureau of Standards, and Association for Computing Machinery)

FOREWORD

This booklet has been prepared for an audience of executives and managers, other than computer and ADP managers, in organizations using computers to help them understand the necessity for computer security and the problems encountered in providing for it.

There are still many gaps in our knowledge. Much more work needs to be done before an organization will be able to implement security provisions which are specific and justifiable responses to defined threats. There are, however, measures which may be taken and this booklet provides a general discussion of those solutions which are available today.

A question and answer format was selected to organize the material in a manner which might logically represent a general approach to analyzing computer security problems. The material in this booklet was drawn from the report of a workshop of top technical experts in the field of computer security, held in December 1972.

The Institute for Computer Sciences and Technology at the National Bureau of Standards, U.S. Department of Commerce and the Association for Computing Machinery. The nation's largest technical society for computer professionals, have been jointly sponsoring¹ a series of workshops and action conferences on national issues. These workshops were designed to bring together the best talents in the country in the respective areas to establish a consensus on 1) current state of the art, 2) additional action required, and 3) where the responsibility for such action lies. The workshop on computer security was the first in the series and did, indeed, establish a precedent of satisfying those goals.

BASIC TERMS

Privacy is a concept which applies to an individual. It is the right of an individual to decide what information about himself he wishes to share with others and also what information he is willing to accept from others. The privacy issue has not resulted from the development of computers, but the heightened interest in it can be laid to the capability of computers for storing vast amounts of readily usable data.

Confidentiality is a concept which applies to data. It is the status accorded to data which has been agreed upon between the person or organization furnishing the data and the organization receiving it and which describes the degree of protection which will be provided.

Data integrity exists when data does not differ from its source documents and has not been accidentally or maliciously altered, disclosed or destroyed.

Data security is the protection of data against accidental or intentional destruction, disclosure or modification, using both physical security measures and controlled accessibility.

¹ The National Science Foundation provided financial assistance in planning the series.

Controlled accessibility is the set of technological measures of hardware and software available in a computer system for the protection of data.

Physical security is protection against physical destruction and theft of assets, including data.

WHY SECURITY?

1. What is computer security?

Computer security refers to the technological safeguards and managerial procedures which can be applied to computer hardware, programs and data to assure that organizational assets and individual privacy are protected.

2. Why should I care about computer security?

Computer data and programs represent an increasingly important part of the assets of every organization in our economy. Every day both business and government become more dependent on computer systems to carry out normal business operations. There are over 130,000 computers installed in the U.S. today representing a current value of \$29.2 billion. There is no way to place a value on the millions of data files and programs used on these machines, or on the value of the services performed by these same machines. Their worth in this sense is clearly inestimable. These assets must be safeguarded.

Consumer and public interest groups as well as individuals are now beginning to demand that their concern for protection of individual privacy be taken into account in the design and operation of modern information systems. The President in his 1974 State of the Union address called for attention to this critical national problem at the highest levels of government. His concerns included modern information systems, data banks, credit records, and electronic snooping as well as ostensibly collecting personal data for one purpose and then using it for another. In fact a number of bills are currently being proposed in the states as well as the Federal legislatures to insure rights of privacy and establish requirements of data protection. Every data processing activity will be impacted by the provisions of the legislation.

Every organization will need to adopt procedures and provide safeguards to protect these valuable assets and meet the requirements of legislation.

3. What must I protect these assets and information against?

Threats to computer system security arise from the unpredictability of environmental conditions and people. Data processing facilities and assets may be protected against natural catastrophe and hostile activity so that the impact on the operations of the organization are minimized. These threats include destruction by environmental forces as well as theft or destruction by individuals. Nature only destroys; man both destroys and acquires. Exposure to these threats creates risk for your organization.

4. Are the threats which can be perpetrated by people on my computer system really serious?

Such threats are very real and serious. Companies have been nearly put out of business by unauthorized manipulation of their data files.

The most common situation is the manipulation of computer system resources for personal gain. Direct physical assaults on computer facilities for purposes of destruction are relatively rare. Nevertheless persons motivated by revenge or antipathy toward modern technology have made direct physical assaults resulting in serious damage.

In a study of computer-related crimes, the significant fact appeared that many people who consider themselves honest citizens who would not steal from other people have no compunction about stealing from a computer because it is a faceless nonentity. The same study revealed that the financial gain from computer crime has little appeal for some people, but they will commit crime for the thrill of "beating the computer".

In reading the following examples, it will be obvious that the individuals involved were apprehended, but it must be assumed that much computer-related crime is not detected and is, in fact, still going on.

a. Internal threat, job related: Because of his familiarity with a bank's programs and procedures, a teller in a New York bank was able to transfer \$1.5 million to his own account without leaving any trace of his activity, completely foiling both automated and manual auditing systems. Authorities became suspicious only when his name was associated with a large betting operation.

b. Internal threat, not job related: An EDP manager and part of his staff used their company computer to "handicap" horse races and pocketed the profits.

c. External threat, computer manipulation: An engineering student discovered a way to gain access to the computerized supply system of a telephone company. He claims to have obtained and sold nearly \$1 million in equipment before getting caught.

d. External threat, forms manipulation: A man substituted deposit slips, magnetically coded with his account number, for the blank ones available on a bank's customer counter, causing the computer to place other customers' deposits in his account. He then withdrew the money and disappeared.

SITUATION TODAY (THE REAL WORLD)

5. Are the main personnel threats to a computer system within or outside an organization?

With question, the "trusted insider" is the greater threat to any computer system. An employee (programmer, janitor, or even manager) with knowledge of the system and its defenses is the most likely to subvert a system. The inept ones are caught immediately, the competent ones may go undetected indefinitely. As organizations place more and more valuable data into large data banks, the potential pay-off for an inside job will get bigger and bigger.

6. Can data in a computer system be completely protected?

No. For every defense there is an alternative offense, but a level of security can be provided that is commensurate with the risk. The desired protection level is that which makes the cost of subverting the system greater than the benefit to be gained by its subversion.

7. Can stored data be secure from destruction or compromise?

Security of stored data depends on the storage media and the threats to which they are vulnerable. There are two types of threats:

- individuals who have physical access to the storage media.
- individuals who have computer access to the storage media.

In the first case, experiments have demonstrated that magnets can destroy data stored on magnetic media, but must be placed in almost direct contact with the medium, e.g. magnetic tape, to cause damage. Physical access to the storage area must therefore be carefully controlled.

In the second case, a user of a computer system can erase data on storage media (either accidentally or maliciously), using the computer. The attack which is most difficult to detect comes from someone who deliberately and surreptitiously modifies stored data for his own benefit.

8. Can commercial computer services be expected to protect data?

To a limited degree and for a price. Computer services usually operate insofar as possible according to guidelines and instructions provided by their customers; special care such as the use of a dedicated computer may be provided for users if requested and paid for. Eventually, the requirement for computer security may create specialized computer facilities which are certified to be secure for specified purposes.

9. Is a dedicated system secure?

A system dedicated to a specific task is more secure than one in which the tasks are still being developed or are rapidly changing. Reservation systems in which the terminal operation has only limited data entry/retrieval capabilities are difficult to probe. The security of such systems depends on careful control of the actions the user may perform; however, the integrity of data in these systems still depends on the integrity of the source.

10. Why don't computer manufacturers "build-in" protective devices and offer total security packages?

Until recently there has not been a general requirement to develop protected computer systems. Hardware and software solutions have not been found for all security problems. However, some protective devices, such as automatic equipment for person identification, will become available, or perhaps even "standard", just as automatic transmissions did in the auto industry. Toward this end, large groups of users with similar security needs, such as the Federal Government, can lead the way by establishing uniform specifications of security for computer systems.

11. Do specifications exist for a secure computer facility?

No specifications exist for a general computer system to achieve a given level of security. Dedicated systems have been implemented to specifications based on restricted security requirements using restrictive solutions. General security solutions may be found for some common problems, but each facility must define its own detailed specifications.

12. Once I have determined requirements for my facility, how can I assure that they are satisfied?

Through compliancy testing. Security features are usually evaluated for completeness, effectiveness, and correctness. Then they are subjected to simulated attempts to breach security. For example, if a security feature of a system is the authentication of remote terminal users through randomly generated passwords which are periodically replaced, then a compliancy test would be a check to see if any of a specified number of randomly generated fake passwords would be accepted. Good design specifications include the range of compliance which will constitute an acceptable test.

13. Can computer security and threats to that security be measured?

Computer security can be measured in terms of the probability that a facility's defenses will be breached by specific threats. For example, the operating system of a secure computer must be designed so that the probability of a penetrator obtaining executive control of the computer system—and thus access to all programs and data—is extremely low. No theoretical methods exist for assigning numerical probabilities to such a situation occurring in the various types of computer systems. Only when a large body of statistics has been accumulated for specific threats can honest numbers be assigned as probabilities. Until then measurement of computer security and the threats to it will be based primarily on intuition and limited experience.

VULNERABILITIES

14. What is the most vulnerable point in any computer system?

Relatively speaking remote terminals are the least secure points of computer system. A system is more vulnerable if it may be accessed from remote terminals both because of the possibility of "bugging" and because remote terminals typically have little supervision. A remote terminal provides a convenient spot from which a would-be penetrator could launch a software attack. This is an attack on a system in which the penetrator gains entry either by simulating another's identity or by using anomalies of the system to probe the hardware and software defenses in order to access unauthorized data or to obtain control of the executive programs. Such an attempt could be disguised as a parametric study of efficiency or other "system" study involving a wide range of hardware and software. Once he finds the key to executive control, the penetrator can compromise any data he wishes and can also erase evidence of his attack and leave a way open for future access.

15. Can a shared system be secure?

Shared systems are currently not secure because of their complexity and lack of cohesive security design. Computers can be shared in several ways with varying degrees of security. In order of increasing risk, some examples of computer systems sharing are:

—Batch-processing systems which sequentially process users' programs while sharing the central processor between a single user and the input/output systems. A user of this system has little control in obtaining others' data while it is being processed but may obtain it

while it is being prepared for processing, either accidentally or intentionally, through his program.

—Multi-programming systems processing several *local* users' programs simultaneously. A user can accidentally access another users' data, but the central processor will not be under his direct control, eliminating most opportunities for deliberate compromise of data.

—Multi-programming systems allowing programs and data to be entered remotely. Such systems are vulnerable to the same threats as a local multi-programming system as well as to threats associated with remote terminals.

—Interactive time-sharing systems processing several users' programs simultaneously. Each user has interactive control over his program and can therefore actively search for other users' data. Some time-sharing systems also allow remote access and consequently are subject to threats through remote terminals.

16. Can communication lines between computers or between computers and peripheral equipment be bugged?

Assuming that "bugging" means the surreptitious attachment of "listening" devices to computer equipment, the answer is, "Yes". The communication lines linking a computer facility with peripheral equipment in other buildings, with remote terminals, and with other computers in a network are highly vulnerable to electronic eavesdropping.

17. Is bugging the only form of electronic eavesdropping?

No. Electromagnetic and acoustic emanations from a computer facility can be detected and interpreted by a listening post outside but in the vicinity of the computer center. However, detecting these emanations is not "bugging" since a listening device need not be attached to equipment or planted within the computer facility. Communication lines, unshielded electromechanical equipment, and CRT terminals can act as signal sources. All such emanations must be suppressed to achieve a highly secure environment.

18. It seems that at present no computer system is secure. If that is true, what can I do?

Although a system which has been designed without security as a prime objective cannot be totally secure, much can be done to improve its security. Systems designed for security are under study now. In the interim, the actions available for improving security fall into two main classes: technical and management solutions.

TECHNICAL SOLUTIONS

19. What are the technical solutions?

They fall into three categories of solutions: computer-based protection techniques, identification techniques, and security audit techniques. All three must be integrated into a secure system according to its security requirements.

20. What are computer-based protection techniques?

They are methods based either on hardware or software, but are in either case an integral part of the computer system design, which per-

form functions such as keeping the data files of different users segregated in a shared system. Some of these techniques are available now such as memory read/write inhibit and segmentation of primary and secondary storage. New programming techniques also permit a compartmentalized approach to data handling.

In systems of the future designed with security as a primary consideration, access to processing resources and data files will be centrally controlled and restricted to a minimum. Design will be based on modular structure in which every module will be like a watertight compartment in a ship; access to one module will not automatically permit access to any others. The barriers between users will be well defined to limit accidental damage and inhibit browsing through another user's files or programs. In addition, technical design criteria for secure systems will include requirements for access controls to be active at all times with no possibility for manual bypassing and for security features to be specified in terms of complete design, correct implementation and proper installation and operation. Data in communication links will be protected, e.g. encrypted.

21. But what can be done now?

In addition to the memory segregation and programming techniques mentioned above, data can be encrypted during both transmission and storage. Encryption also known as scrambling, is the most inexpensive way of protecting data travelling over long distances from electronic eavesdropping. It is also effective for data in storage or in memory in a shared system. However, it is a method of protection especially subject to internal subversion; its success depends on the security of periodically changed keys. The keys are only as secure as those who have knowledge of them.

22. How can data integrity be determined and maintained?

Data integrity may be verified by checking the data or its representation against something known to be accurate. At one extreme, this means checking it word for word against its source. If the source is on tape or in some other machine readable form, the checking can be done by computer, but it is still expensive and time-consuming.

Problems may also be discovered by analyzing systematic errors, trends, and error frequency, but more popular is the use of error-detecting bits, which produce error "flags" when the sums of the data being used do not check with the equivalent sums in the original data. "Bounds controls" are useful because they can sound a warning when data items are not within certain limits, e.g. an inordinately large check is being issued by a payroll program. Data integrity can also be maintained through redundancy, either by having duplicate copies of the data or by processing the same job on different machines.

23. What are the identification techniques?

Identification is simply the recognition of an individual, a program or a set of data from a name or identification code. Authentication is the verification of identity—a double check, so to speak. Authentication may require that the user supply his unique password or enter his unique key-card. Authentication may even involve physical verification of the claimed identity.

24. How does a computer system automatically and reliably verify legitimate users?

A computer system can verify a legitimate user in three ways:

a. From his knowledge of a password, phrase, number or other privileged information. Passwords are widely used today. They are, however, rather easily obtained by unauthorized persons either from those knowing them or from their notes and printouts, or even directly from the computer memory.

b. From his possession of a unique physical key, such as a card containing unique information. Such physical items, however are easily lost, stolen, or counterfeited.

c. From automatically measured biometric data, such as hand geometry, fingerprints, voiceprints, etc. These biometric methods promise high reliability and accuracy, but most techniques are still in the research stage.

25. What is meant by security "audit"?

Computer system auditing involves an independent and objective analysis of the security of a computer system. A security audit determines the adequacy and effectiveness of system controls vis-a-vis their threats. It includes both scheduled evaluations and after-the-fact investigations of attempted penetrations of the computer system. An automated, realtime audit mechanism can often provide a timely alert of penetration attempts. Whether after-the-fact or real-time, the auditing procedures should provide sufficient information for damage assessment and for purposes of prosecution.

26. What is an "audit trail"?

An audit trail is a record of what processing is being done to specific data and programs in the systems and by whom. To be useful this record should be organized (preferably automatically) into reports of the following types:

- Alerts of possible security violations.
- Review of system activity.
- System security status summaries.
- Damage assessment reports.

27. Who should do the auditing?

Both internal and external auditors should be employed. Both should audit some of the same systems so that results can be compared directly. It is important that internal auditors occupy a neutral position as high in management as possible, i.e. they should not have any responsibility for ADP operations.

MANAGEMENT SOLUTIONS

28. What are some management solutions?

Planning, funding and implementing security solutions are fundamental management actions. In particular, the areas to be considered include physical security planning, personnel selection and education, system selection and procurement of computer system security options, security certification and provisions for computer operations security. Controls used to achieve computer security must be uniformly en-

forced because of the value of the commodities and assets being protected; this is the reason for total management involvement.

29. What are specific management steps that can be applied to improve computer security planning?

First, appoint an independent manager of computer system security, i.e. other than the ADP operations managers, with direct authority in security matters. Then organize a computer security program and conduct a risk analysis. The security program should make provisions for:

- Specifying precisely who can read, use, or modify data. Ensure that technical as well as administrative controls are used to implement these instructions.

- Conducting independent internal and external audits.

- Keeping accurate and up-to-date organization charts, delineations of responsibilities, and work statement.

- Maintaining and promulgating thorough and detailed plans for normal operations, emergency operations, and recovery operations.

- Motivating employees to report insecure practices or suspicious activities, as well as to maintain their own security awareness.

30. What kind of physical protection should be considered for a computer facility?

The first line of defense consists of good engineering management:

- Locate in areas not exposed to floods, wind, high tides, fire, etc.

- Construct a facility which can be easily guarded.

- Ensure that electromagnetic emanations are minimized.

- Install emergency power sources, water pumps, airconditioning, etc.

- Provide adequate emergency maintenance facilities.

- Operate the facility to ensure personnel safety.

- Provide backup or data for data processing.

31. What personnel selection procedures are necessary beyond normal hiring practices?

Perhaps none if present practices include a comparison of the candidates' previous salary with his present standard of living and personal wealth (or debts) and careful verification of previous employment records, character references and reasons for leaving.

32. What educational programs are needed in security?

Security education and training should not be a one-time thing. Refresher courses and periodic security reviews should be required for all personnel. In addition to the basic indoctrination, the following should be considered:

- Handbooks with security rules and penalties for their violation fully and clearly specified.

- Educational and motivational posters.

- Dissemination of some (but obviously not all) of the security measures in force at your facility.

—Publicity for selected cases of computer abuse at other installations when the penalties imposed were severe. Details of perpetration should be omitted, however.

33. What is security "certification"?

Certification is a managerial declaration that the security features of a computer system comply with the specifications which, in turn, satisfy the security requirements. The details of technical analysis leading to security certification are not well specified at this time and there is no certifying agency, as such. However, some prerequisite actions necessary to this process are:

- Modeling of the system and the analysis of the model.
- Formalization of the access controls.
- Prediction of system security degradation and its effect.

Certification should take place at discrete points during the design, implementation, and operation of a system, viz.

- To check that the design is complete.
- To confirm that the implementation is correct.
- To determine that the installation meets all design modifications.
- To determine that the installation meets all design standards and requirements.
- To establish that a system is secure after system modification, failure or penetration (either detected or suspected).

34. What steps should be taken after a penetration is detected?

The status of the system's security must be analyzed to determine which portions have been affected and what has been lost. The unaffected portions may then be restarted, but it is crucial not to overlook any program modifications the penetrator may have left behind which permit easy re-entry at a later time. An important factor in computer system recovery is the existence of a reference point. A reference point is a backup set of key programs and data bases—certified to be correct and unmodified—stored at another secure location. With such a reference point and using operations logs and files, the step-by-step recovery and recertification of other programs and data bases can begin. Care should be taken that the access point through which penetration occurred is fully covered in the restored system.

35. What are the costs of providing computer security?

The costs of providing computer security may be broken into three areas: initial cost, operational cost, and overhead cost. The importance of information processing in the business and governmental communities makes the assumption of these costs mandatory at a level commensurate with the risks to the system. At a minimum, this risk is equivalent to the value of the computer equipment.

Initial costs include:

- Physical security equipment controlling personnel access to the ADP facilities.
- Physical security equipment protecting data in storage.
- Additional equipment for identification, data encryption, program isolation, and security auditing.

—Operating system modifications and additional software needed to utilize this equipment.

Operational costs include:

- Salaries of security personnel.
- Maintenance of security equipment.
- Creating and updating user authorization lists, data file descriptions, data encryption keys, and data access records.
- Security training for operations personnel.
- Certifying and auditing system security.

Overhead costs include:

- Impact on computer system efficiency and flexibility.
- Impact on personnel attitudes.

36. What benefits may be derived from computer security?

The costs incurred in providing computer security must be placed on perspective to the benefits gained by providing it. These benefits include:

- Protection of individual privacy by compliance with security requirements of Federal and state legislation, management policy, and user confidentiality agreements.
- Protection of the physical assets of the computer facility.
- Protection of the financial investment in programs and data.
- Protection of the assets represented by data.
- Better system and data integrity.
- Better reliability and timeliness of data processing.
- Better accounting of data and resource usage.
- Better employee awareness of their importance to the organization.

SUMMARY

37. What priority should be accorded the various measures suggested for improving computer security?

The first step in computer security is simply controlling personnel access to the computer facility. Creating and maintaining a "security environment" will let both employees and outsiders know that safeguards exist.

Next come some administrative measures:

- List hardware and software resources (including data bases) in order of value.
- Perform a risk analysis.
- Formulate the goals of the security program.
- Determine the investment required to counter the estimated threats.
- Create a security organization, assigning it fully responsibility for security.
- Plan a security program and implement it.

The order of priority for the next steps depends upon the cost/benefit studies. A common pattern might be:

- Upgrade the initial physical security measures.
- Establish personal identification systems and other controlled accessibility procedures.
- Control the flow of data throughout the processes of collection, entry, storage, processing and dissemination.

- Make individual users personally accountable for control of, and access to, data.
- Implement software security to the degree indicated by the cost-benefit analysis.
- Shield the facility against electromagnetic leakage.

[From the Washington Post, Oct. 6, 1974]

PROTECTION FOR COMPUTERS GROWING

(By Martin Skala)

New York—In an effort to reduce white-collar crime and safeguard business records, security-conscious companies are throwing a protective net over their computers.

The corporate computer center, with its blinking lights and whirring tapes, is no longer considered a glass-walled showcase for all to see. Instead, computer-security experts say, business firms are increasingly limiting physical access to costly data-processing centers and taking special measures to protect computer files.

Concern over computer security has grown considerably since disclosure of the Equity Funding scandal and other less spectacular cases of computer fraud, according to Joseph Wasserman, president of Computer Audit Systems.

As more companies process their records by computer, he says, the risk of major losses, either through fraud or human error, mounts substantially.

This computer-security expert says that companies must be alert to several types of computer misuse, ranging from vandalism by disgruntled employees to the theft of money or proprietary data by covert manipulation of computer files.

But Wasserman said programming errors and poor controls cost businesses far more than do deliberate attempts to steal.

Programming errors can destroy, scramble, or misplace data, resulting in thousands of dollars of financial loss, if managements don't install proper controls.

In one widely reported case, an inexperienced programmer had made a key change in the accounts-receivable file of a large retail chain which was responsible for destroying, by erasure, all customer-debit balances, and led ultimately to the chain's bankruptcy.

This type of problem, Wasserman said, can be reduced by using the technical capabilities of the computer to audit itself.

To protect computerized data against tampering and to spot errors, Computer Audit Systems and other computer consultants have devised special computer programs for control purposes. These consist of series of instructions, written in computer language, that independently analyze information already processed by the computer.

The audit software, in effect, tests the information stored in the computer for accuracy and, in some cases, may even detect fraudulent acts.

In addition, many computers are being programmed to limit an individual's access to certain files. Sometimes passwords, keys and badges are required to activate a computer-input device, thereby limit-

ing access to the system. Some business firms, Wasserman said, instruct the computer to produce a journal, or log, which reveals who has used the system, when, and how.

Major accounting firms, some of whom faced legal suits because of alleged oversights in detecting computer fraud, are rapidly building up computer-auditing expertise.

[From Business Week, July 28, 1975]

ESPIONAGE IN THE COMPUTER BUSINESS

George Foldvary, executive vice-president of Keronix, Inc., was quietly celebrating his 51st birthday with a woman friend at a Los Angeles restaurant on Jan. 3, 1973, when a business associate phoned to tell him there was a fire at the plant in Santa Monica. Figuring that it was a ruse to lure him to a surprise party, Foldvary, still wearing his dinner jacket, drove to the plant, ready to swing. But when he arrived, he found that the fire report was no joke.

Fire officials and insurance investigators quickly diagnosed arson. Keronix Chairman Laszlo Keresztury, 40, like Foldvary a Hungarian immigrant, became impatient with local police efforts to identify the culprit and hired a private investigator. The detective's findings caused Keresztury last December to file a suit that shook the entire computer industry.

Tiny Keronix, a privately owned manufacturer of minicomputer core memories whose \$3.5-million sales in 1974 make it a mere blip in the \$1.25-billion minicomputer industry, charged Data General Corp. of Southboro, Mass., an industry leader, with an elaborate conspiracy to put Keronix out of business. The suit alleges that these machinations ultimately led to the fire. Keronix asked \$5-million for interruption of business and \$50-million in punitive damages.

Data General's young entrepreneurs, who in just seven years have built their company from nothing to sales of \$83.2-million, angrily denied the allegations and answered the Keronix suit in kind. Their countercomplaint charged Keronix with pirating trade secrets from Data General. "Keronix and its agents," it said, "obtained such proprietary material by, among other methods, purchasing Data General equipment and in connection with the purchases obtaining such proprietary material, which is furnished by Data General to its customers."

FAIR-WEATHER FRIENDS

Pressuring of customers and industrial espionage are not uncommon in the fiercely competitive minicomputer industry, which is only 10 years old and still in its rough-and-tumble formative stage. One measure of how much investors distrust the industry is the refusal of some to dismiss the seemingly far-out suggestion that big and successful Data General might really have had something to do with the fire at tiny Keronix. When the Keronix suit was made public last January (page 62), Data General's stock, always among the more volatile issues on the New York Stock Exchange, dropped to less than 9. Even the institutions, which have been friendly toward Data Gen-

eral, grew nervous. The biggest seller in January was said to be Keystone Custodian Funds of Boston, which reportedly sold 300,000 shares at an average price of about \$9 per share. Since then, DG's stock has rebounded and is now trading at about \$35 per share.

While Keronix and Data General exchanged civil suits, a federal grand jury in Los Angeles spent nearly two years pondering the criminal aspects. On June 30, a gleeful Data General issued a press release reporting that federal authorities had told the company that the investigation had been terminated and that no federal indictments were forthcoming.

The DG release was accurate but incomplete. As Vincent J. Marella, Assistant U.S. Attorney in Los Angeles, describes what happened, "We are declining prosecution and referring the case to local authorities because we have limited statutes." This means that the Los Angeles district attorney will inherit the grand jury files and can pick up where the grand jury left off.

Meanwhile, the two companies have been lobbing allegations at each other, Keronix claiming that Data General wants to put it out of business, DG charging that Keronix is simply running a huge publicity stunt. The battle has been joined by a phalanx of high-priced lawyers. At least eight private detective agencies have at various times been hired by one side or the other, and local, state, and federal agencies have been drawn into the fray.

ANTAGONISTS

Keresztury, who owns 46 percent of the stock in Keronix, used \$10,000 of his savings to incorporate the company he started in a spare bedroom six years ago. He had fled Hungary in 1956 and after attending the University of London came to the U.S., where he worked for Ampex Corp. and later Teledyne, Inc. There, he says, he "designed computer memories that are still being used today."

Data General, on its part, accounts for 10.7 percent of worldwide shipments of minicomputers, according to a survey by Modern Data Services, Inc. That makes DG No. 2 in the industry, a long way behind Digital Equipment Corp. (DEC), which holds 33.6 percent of the market.

Data General grew out of DEC. In 1968, Edson D. de Castro, then 30, quit his systems engineering job at DEC's Maynard (Mass.) headquarters to form DG in neighboring Southboro. Some of his associates were even younger than de Castro, who became president. For financing, they turned to New York attorney Frederick R. Adler, who raised capital and was an initial investor. Adler, then 43, was the old man among the youthful organizers. He became secretary and a board member.

No sooner had DG begun producing its Nova series of minicomputers—in direct competition with DEC's immensely popular PDP-8 line—than even smaller companies began duplicating the product. The big mainframe-computer manufacturers had long since learned to live with this kind of problem, but it was new to the infant minicomputer industry, and de Castro reportedly was enraged by what he viewed as thievery.

Typically, the supplier of a computer provides the buyer with manuals that not only describe the hardware but also spell out the software—the list of instructions that tell the computer what to do. Small, low-overhead companies have been known to use the data in these blueprints to duplicate the hardware of major companies by a process called “reverse engineering.”

Once it knows how the original was built, a small company can begin to make replacement parts and peripheral equipment that fit the system and can be operated by the original software. These companies can almost always do the job cheaper than a big computer maker can because, as Donal W. Fuller, chairman of Microdata Corp., another minicomputer maker, explains, “they don’t have the marketing, product development, and software overhead costs.”

They must be careful not to infringe on patents, which the big companies use increasingly as a defense. And there is the murky area of trade secrets which, although not patentable, may be considered privileged. Reverse engineering “is fairly new in the minicomputer industry, but it is fair play,” says Microdata’s Fuller. “Keronix does it to Microdata, too, but we don’t sue.”

DRAWING THE LINE

De Castro is not so patient, though, and he has not hesitated to sue. His battles with Keronix began more than four years ago when DG’s Los Angeles law firm, Keatinge, Libott, Bates & Pastor, hired California Attorneys Investigators, Inc., to learn if the Santa Monica company was stealing secrets from DG. In a confidential report dated Sept. 1, 1971, the detectives said: “There does not appear to be explicit subterfuge or espionage occurring between the subject company and the competitive computer companies, including client company.”

DG was unhappy with California Attorneys’ conclusions, so in May, 1972, the management hired Dan Sullivan, a Boston detective who had been used by a DG executive in a divorce fight. According to attorney-investor Adier, Sullivan’s assignment was to look for leaks within DG. “We wanted to know if any employee of DG was selling trade secrets, with particular emphasis on Keronix,” says Adler.

In a month on the job, Sullivan apparently found little evidence of leaks from within DG, so the investigation again turned to Keronix. Sullivan hired a Los Angeles private detective named Robert A. Clark to carry out the West Coast snooping. Clark attempted unsuccessfully to tap Keronix’ telephone lines, according to the Keronix suit. Next, says the suit, Clark and two associates “fraudulently” obtained Keronix telephone bills from General Telephone Co.’s office in Santa Monica.

The detectives were trying to learn which DG customers were also doing business with Keronix. This could lead them to companies that were passing DG manuals on to Keronix, enabling Keronix to do “reverse engineering” on DG products and to undercut DG’s core memory prices. Pressure was then allegedly brought to bear on these customers by DG’s marketing operation.

Adler, speaking for DG management, refuses comment on the telephone bills. Nor will Richard Bates, a partner in DG’s West Coast

law firm. But he does allow: "You can obtain phone records of anyone for a small payment. It might be illegal for the phone company or phone company employee to give them. But it is not illegal to get them."

PRESSURE ON CUSTOMERS

Laszlo Keresztury says that he was puzzled at the time by the number of calls he got from customers complaining that DG had learned that they were doing business with him. But he gives only a few examples because, he claims, his diary was destroyed in the fire.

Clinton Day, vice-president of Beehive Medical Electronics in Salt Lake City, says that a DG agent made some "mild threats" and "threatened to sue us if we continued dealing with Keronix." According to Day, the DG sales agent also "implied that DG had industrial spies that were keeping Keronix under surveillance."

Another DG-Keronix customer, Frederick J. McKee, vice-president and general manager of M&M Computer Industries, Inc. a Singer Co. subsidiary, says: "Data General is a very tough competitor, and they can be very heavy-handed."

Keronix' suit claims, however, that the sleuthing done for Data General by Sullivan, Clark, and others went far beyond obtaining telephone bills and pressuring Keronix' customers—and indeed led directly to the fire. But Adler of Data General says that DG finished with Sullivan's services in August, 1972—and the fire at Keronix took place five months later.

THE ARSON JOB

There was no doubt that the fire was the work of an arsonist. Keronix' insurance carrier, Insurance Co. of North America, hired Jasich & Lowe, Los Angeles fire investigators, to look into the fire. It turned out that fires had been set in Keresztury's desk and in the blueprint room, says investigator Thomas Pugh. The locations of the fires led to suspicions of espionage.

Oddly, in forcing a shipping door open with a truck, the arsonists did not set off the ultrasonic burglar alarm system. And even though there was plenty of expensive equipment about, all that was stolen were a typewriter, an adding machine, and a six-pack of 7-Up.

Months later, the Los Angeles County sheriff's staff found a "fence" who was trying to sell the typewriter. The investigators traced the typewriter back to a man named Ralph A. Zoebisch, who was on probation after a conviction for receiving stolen property. Zoebisch, who is identified in the suit, says that he told the Federal Bureau of Investigation and the Santa Monica police that he worked in the shipping department of a company next-door to Keronix. He told the Santa Monica police that Clark had offered him \$300 in advance and \$200 upon completion for setting the Keronix fire. Zoebisch, who has since been charged with possession of stolen property, said that to make it look like a burglary he took a few items.

Zoebisch repeated these statements this week in an interview with *Business Week*. "It was a business deal," says Zoebisch. "Clark told me what he wanted done. When you do something illegal, they don't tell you why, and I don't ask questions."

Zoebisch also told how, at the behest of a detective working for Keronix, he had identified Clark as the man who had paid him for

the arson. He said he pointed Clark out in the crowded lobby of a Los Angeles office building. A police source says that Zoebisch also identified Clark's photograph.

A STORY ATTACKED

The Zoebisch story has been under attack by DG's West Coast attorneys, who hired yet another private detective agency, this time the internationally known Intertel, Inc. An Intertel detective, along with Robert Clark, went to a California prison camp where the fence's brother was serving time for possession of marijuana. According to Santa Monica police sources, the fence is important because he can confirm the Clark-Zoebisch tie, as stated in the Keronix suit.

DG attorneys now say that the fence is recanting some of his claims to the police about the fire. Keronix and Zoebisch argue that this took place after the prison farm visit because the detectives threatened the fence and his family.

Intertel detective Albert A. Murphy would not comment on the allegation. DG lawyers and Clark deny it. Calling the prison-farm story "ludicrous," Clark claims not to have met Zoebisch or the fence until 1975, two years after the alleged arson.

Keronix suggests in its suit that Data General sought to hide payments to Clark and his West Coast team by using a company called Chris D. Christimirk as a conduit. The implication is that this company "laundered" the money.

No company of that name exists, but a now-defunct Boston collection agency was named Christimrick. It was founded by Barry Haraden, a Boston insurance man, and its strange name was coined from his sons' first names—Christopher, Timothy, and Patrick. But Haraden claims that he does not know any of the DG defendants and says: "I couldn't even launder my own shirt."

Haraden acknowledges that he did send Clark two checks, each for \$1,000. But he claims that he did this to help out DG's detective, Dan Sullivan, who, he says, was having financial problems and could not afford to pay Clark directly. Sullivan, he says, was a friend and a former employer of his wife.

WHOM TO BELIEVE?

As the case has dragged on from months into years, it has become mostly a question of whose detective you believe. Data General, for all its success and sophistication in making minicomputers, has used one detective after another in looking for evidence against Keronix. And the crux of DG's countersuit is that Keronix' private detective, who dug up all the dirt on DG's detectives, is himself a tarnished individual with a criminal past.

The countersuit says that this detective has "publicly admitted that he has committed the crimes, among others, of perjury, subornation of perjury, embezzlement, bribing officials of the City of New York . . . labor union officials . . . [and] is an admitted associate of known underworld figures."

Once known as Herbert Itkin, the detective was for 20 years an undercover agent abroad and in the U.S. for the Central Intelligence

Agency and the FBI. He was a lawyer with a long list of mob clients, and his testimony helped send two leading New York politicians and more than a dozen organized crime figures to prison.

In 1972, the Justice Dept. set him up on the West Coast with a new identity, and his new name—as well as his old one—was revealed in the Data General countersuit. As it happens, a New York lawyer, Robert Morvillo, who handled the criminal aspects of the case for Data General, was formerly head of the frauds section in the office of the U.S. Attorney for the Southern District of New York. Itkin was his star witness in a number of criminal prosecutions, and Morvillo was among the people who arranged Itkin's new identity. Morvillo dropped out of the Justice Dept. for a time, worked for Fred Adler's law firm, returned to the government, and in 1973 left again to start his own practice. One of his first cases was to advise DG executives in connection with the grand jury investigation into the Keronix fire.

Morvillo heatedly denies that he ever informed DG's executives or its other attorneys of Itkin's history. He claims that he did not know for six months that Itkin was involved, adding: "I completely isolated myself from the civil suit."

When asked where Data General learned about Itkin's new identity, Fred Adler said: "I'm not going to tell you where we learned it. It was not a well-kept secret on the West Coast. To the best of my knowledge, the information did not come from Morvillo." Clearly, Data General plans to make Itkin's past an integral part of the present suit against Keronix. What DG does not say in ticking off Itkin's criminal activities, however, is that the acts were committed in the service of the U.S. government.

Chances are the fight between big DG and tiny Keronix will continue for years. The criminal investigation, after being stalled in a grand jury for two years, now may be opened anew by the Los Angeles district attorney.

As for the civil case, neither side shows any sign of moving toward an out-of-court settlement. Says Laszlo Keresztury of Keronix; "This whole thing is a pain. But if I let it pass by, I couldn't look at myself. I am too stubborn or too Hungarian." Snaps Fred Adler of Data General: "If I thought someone in our company did something wrong, I'd have settled a long time ago. But this is blackmail, and I don't pay blackmail."

[From the New York Times, Apr. 3, 1976]

TAPPING COMPUTERS

(By David Kahn)

GREAT NECK, N.Y.—Like people, computers talking to one another can be wiretapped. To protect themselves, more and more companies, such as the oil giants and banks, are putting their digital correspondence into secret form.

This has led to a demand for a common cipher—a system that would both permit intercommunication among computers and safeguard the privacy of data transmissions. The National Bureau of Standards,

with the help of the National Security Agency, the Government code-making and code-breaking body, has proposed one.

The interesting thing is that while this cipher has been made just strong enough to withstand commercial attempts to break it, it has been left just weak enough to yield to Government cryptanalysis.

Under the plan, all participating computers would incorporate the cipher hardware—tiny integrated-circuit chips, each mounted on an inch-long plastic wafer. For privacy, each pair of correspondents would have an individual key—a string of zeroes and ones, each string different.

The sender would use this to put outgoing messages into cipher; the recipient, to decipher incoming texts. Competitors would not be able to use their keys to unlock these messages any more than your neighbor's house key will open your front door. And even if a competitor has somehow gotten hold of an original message, so many keys are to exist as to make it impractical for him to find the right one and so uncover other messages enciphered in it.

Each individual key in the cipher as proposed would have 56 zeroes and ones, or bits (short for "binary digits"). This length, two computer scientists at Stanford University say, has been craftily chosen to make it too expensive for private firms to cryptanalyze the digital messages—but not for the Federal Government.

Prof. Martin E. Hellman and a graduate student, Whitfield Diffie, suppose that someone wanted to crack these messages by "brute force"—that is, by trying all keys possible for a particular situation. This someone could build a computer using a million of the chips. It could test a trillion keys per second. With 56 bits, the total number of possible keys is 70 quadrillion. The computer could thus exhaust all keys in 70,000 seconds, or less than 20 hours.

In large quantities, Hellman and Diffie say, the chips would cost perhaps \$10 each at today's prices. To design and build a million-chip machine would come to about \$20 million. If this were amortized over five years, the cost of each day's operation—in effect, the cost of each solution—would amount to about \$10,000.

Who, they ask, has the money to spend on such a machine and the need for daily solutions that would justify it? Only the Government. For private industry, the gains would hardly be worth the investment.

Now suppose the key length were 48 bits. The price of a machine to generate a solution a day would fall to \$78,000 and the cost of each solution to \$39. On the other hand, if the length were 64 bits, the price of such a machine would soar to \$5 billion and of each solution to \$2.5 million. This seems beyond even the bottomless pocketbooks of the intelligence agencies.

The National Security Agency and National Bureau of Standards argue that the two men's assumptions are off and that people wanting this information would find cheaper ways to get it than by breaking codes. But just because a house has windows is no reason for not locking the front door, Hellman and Diffie reply, and computer security experts at International Business Machines, at Bell Telephone Laboratories, at Sperry Univac, and at the Massachusetts Institute of Technology agree with them that 56 bits is too small. Indeed, one major New York bank has decided not to use the proposed cipher, called the

"data encryption standard," in part for the same reason. And the House of Representatives Government Information and Individual Rights Subcommittee is now looking into the matter.

Hellman and Diffie urge a key length variable at the will of the user up to 768 bits, which they claim can be done at a negligible increase in cost. This would render messages insoluble forever, despite the continuing drop in computation costs.

Why should the National Security Agency be so passionately interested in the 56-bit key that it asked to attend a meeting that Hellman set up on the question and flew a man across the country for it? The N.S.A. expert declined to say. But one obvious reason is that, with a solvable cipher, N.S.A. would be able to read the increasing volumes of data that are flowing into the United States time-sharing and other computer networks from abroad.

The problem is that it would gain this information at the expense of American privacy. For it would also be able to crack domestic computer conversations as well as masses of enciphered personal files. And recent history has shown how often an agency exercises a power simply because it has it.

But perhaps the intelligence is worth it? The answer to that was given a long time ago. "For what shall it profit a man if he shall gain the whole world and lose his own soul?"

David Kahn, a journalist, is author of "The Codebreakers."

[From the Washington Star-News, Apr. 7, 1974]

THE NEW COMPUTER CROOKS: THE INTRICATE SCHEMES THAT NET MILLIONS

(By T. K. Irwin)

One morning not long ago, an unidentified man walked into a Washington, D.C., bank, deftly pocketed deposit slips at the writing counters and replaced them with his own electronically coded forms. In the next three days customers who came in without a personal deposit slip used those "blank" forms. Through a computer, their deposits went into the invisible bank robber's account. On the fourth day he withdrew over \$100,000, vanished, and still hasn't been caught.

That elegant caper is but one of a mounting number of computer-assisted crimes involving uncounted millions of dollars in cash, goods and services. In this latest sophisticated crime wave, most of the victimized banks, corporations and computer companies don't report their losses because they're reluctant to encourage more. Yet in a study for the National Science Foundation, the Stanford Research Institute has collected a file of at least 150 known major computer "abuses" in the past three years, averaging about \$1 million per crime.

"Business has probably never been so vulnerable to theft," warns Donn B. Parker, a Stanford senior computer specialist.

What can the wizards of the electronic underworld steal through computers? Besides embezzlement of cash—the most common loot—they have purloined trade secrets and computer programs (software)

for resale. Some obtain accounts and mailing lists for a firm's competitors. Others have utilized the Brain to disguise their own fraudulent practices.

Hidden among the 2,230,000 people working with the nation's 140,000 computers, the new breed of thief represents the elite in the criminal hierarchy. Typically, he is under 30, very bright, probably armed with a degree in advanced electronics and ready access to a computer. Challenged by the notion of "beating" a complex systems, he is apt to rationalize that stealing from a bank or giant company is not really "illegal."

Experts say that an electronic system is an easy tool for "breaking and entering" because it does what it's told and can be programmed to cover the thief's tracks. As the intricate computers perform faster and faster, telescoping several bookkeeping operations into one, fewer details appear on print-outs (printed records of the computer's activities). Thus, if a thief changes a program to include, say, a \$50,000 phony payment to an accomplice, then switches the program back to its original, there would be no printed evidence of the bogus item that can be traced.

Also, so much record keeping is centralized in a computer's brain that a talented larcenist can pull off a sizeable haul with only a few seconds at the machine and the ability to instruct it.

A wide variety of ingenious techniques have been resorted to a fooling the Brain. Some prime examples:

In Salinas, Calif., an accountant plundered \$1,000,880 from his company during a six-year period by recording in the computer higher payments for raw material than his company actually paid. Craftily, the accountant had the computer assign the extra cash to his own dummy firm.

Last year, a chief teller at a New York savings-bank branch was charged with salting away more than \$1.5 million from the bank's deposits. He was said to have cleverly shuffled hundreds of inactive accounts, feeding false information into the bank's computer so that the accounts always appeared up to date whenever quarterly interest payments came due.

Incredibly, someone was able to manipulate Penn Central Railroad computers to divert 277 freight cars, worth \$1 million, to a small Illinois railroad and hide them there.

Every weekend a quiet employee in charge of computer cards at a brokerage firm went to his office. There, he arranged for computers to gradually transfer \$250,000 from his company's account to his wife's account by showing the money had been used to buy stock. This went on for eight years, and the employee was even promoted to vice president before his filching was discovered.

Unquestionably the most spectacular case of swindle-by-computer was the infamous Equity Funding Corporation case last year. Over \$2 billion in dummy life insurance policies on nonexistent persons were artfully programmed into company computers, and tapes printed out sham assets, all accepted as legitimate by auditors. "Policies" were sold to other insurance companies for cash. To cover up the hocus-pocus further, fake death certificates were programmed into computers. Clearly, those magical machines

turned out to be the key flimflam implements, used by Equity executives on a grander scale than ever before.

What's disturbing about data-processing companies and big business is that fraud is so hard to detect. In the Equity Funding fiasco, the scandal exploded only after a former employee tipped off a Wall Street analyst. Usually, culprits are uncovered merely by accident rather than by audits. The New York savings-bank embezzlement, for instance, popped up after a police raid on a bookie joint. The police found records showing the chief teller had been betting as much as \$30,000 a day. That led to his undoing.

One Minneapolis programmer had siphoned off a small fortune from a bank by having the computer ignore overdrafts in his own account. This speculator was apprehended only because the computer broke down and the bank's accounts had to be checked manually.

How to prevent such automated ripoffs? Not surprisingly, the menace has generated a data-security industry composed of about 20 private companies, and IBM has launched a \$40 million research program to thwart frauds. All kinds of gadgetry and computer "audits" have been introduced in efforts to make the machines crime proof.

A top computer manufacturer, Honeywell, Inc., recently devised a scheme called Multics that restricts the total amount of information available to any user. In addition, every person with access to a computer will have to identify himself by a combination of passwords and project numbers. "We're plugging some of the holes in the old system," says Jerry Lobell, manager of Honeywell's data-security task force.

Still, according to Stanford research engineers, it will take at least five years, maybe ten, to develop wholly invulnerable systems. Meanwhile, smart crooks keep honing their skills. Convicts can even enroll in helpful computer courses offered as job training in many prisons.

On the bright side, there's the curious case of Jerry Schneider, a 25-year-old engineer who concocted a gimmick for ordering expensive equipment from a West Coast company through its computer by punching the right beep tones on his own touch phone. In three years he acquired about \$1 million worth, setting up his own business to sell the loot—until a disgruntled confederate blew the whistle that landed Schneider in jail.

Out on probation, Jerry Schneider has gone legitimate, now counseling clients on how to safeguard their computers against illegal entry.

[From Saturday Review, Nov. 15, 1975]

THE TROJAN HORSE CAPER—AND ASSORTED COMPUTER CRIMES

(By J. Taylor DeWeese)

At 19 Jerry Schneider was president of his own thriving electronic-equipment business, Creative Systems Enterprises. The "creative" aspect of the business was that the equipment he sold belonged to the Pacific Bell Telephone Company.

Posing as a magazine reporter, Schneider toured Pacific Bell's computer installation; he asked a lot of questions and pocketed a handful

of discarded punch cards. Armed with this information, his basic high-school knowledge of computers, and a touch-tone telephone, the teenager keyed into Pacific Bell's inventory-and-supply computer and robbed the company blind.

Schneider's swindle worked this way: he knew that the company's huge main computer was connected, via telephone lines, to a series of outlets called "terminals," which were located in the various branch offices. These terminals look like outsized typewriters; by punching the keyboard, anyone who knows the codes can ask questions of the computer and get back quick answers, and can order the computer to send commands or messages to other units within the system.

Schneider would simply tap in on one of the computer-terminal phone lines and, posing as a company executive, would order the computer to arrange after-hours delivery of a huge consignment of equipment, to be sent to a remote phone-company warehouse. Creative Systems trucks would then pick up the equipment before phone company employees arrived for work the following morning. Finally, Schneider would order the computer to destroy all traces of the phony order and delivery.

The Pacific Bell caper is not an isolated instance. In the first six months of last year alone, authorities discovered more than \$27 million in embezzled funds, misdirected assets, purloined programs, and unauthorized computer time involving companies nationwide. Computer fraud is rarely detected by conventional auditing and is usually discovered by sheer happenstance; today's reported cases represent only the tip of the iceberg.

Computer crime is, in short, big business. The question is, Whose business is it? Is the computer crime wave the cumulative product of small-time heists engineered by various disgruntled employees, financially pressed programmers, or sporting "computerniks" bent on beating the system? Or has large-scale organized crime co-opted the computer?

The evidence on this point is sparse but indicative. At least two instances of Mafia involvement have surfaced to date. A California computer programmer who fell behind in his gambling debts was forced to disclose sensitive programs to organized crime figures and to cooperate with them in a computer looting scheme. In another case the FBI found that a major Midwestern bookmaker was using unauthorized computer time on a local university's computer system to calculate his handicaps!

Justice Department officials nevertheless tend to downplay the role of organized crime in computer finagling. The Mafia prefers to focus, the department says, on their straightforward and high profitable gambling, prostitution, drug, and loan-shark operations.

Obviously, computer crime has many dimensions. At one end of the scale, there is the young systems analyst, at a Midwestern bank, who programmed the bank's computer to ignore his \$300 "rubber" check. At the other extreme is the \$2 billion Equity Funding scandal, which saw thousands of stockholders and some of the most sophisticated institutional investors on Wall Street duped by a financial empire built on phony computer printouts.

Not long ago an astute bank customer exchanged the blank deposit slips on the bank's service counter for his own magnetically encoded

slips. The bank's customers unwittingly filled out his slips, thus depositing their funds into his account, because the computer ignored the depositors' handwritten numbers in favor of the pirate's magnetically encoded digits. A more sophisticated heist involved a bright young computer executive who broke the code of a rival time-sharing company and looted his victim of some 5 million dollars' worth of classified customer programs.

Occasionally, the computer is an accessory "before the fact." One chief accountant, who embezzled \$1 million during a period of six years, used his employer's own computer to build a model of the company's financial operations. The model gauged appropriate changes in accounts receivable and accounts payable that would remain undetected in auditing. For example, if an inventory shrinkage of 5 percent was common, then phony orders and payments up to 5 percent of accumulated inventory would go largely undetected. So, within the indicated limits, the accountant stole assets to his heart's content. In a somewhat similar case, a very efficient burglar browsed through computerized credit reports to locate victims who were "loaded."

Despite the many variations in technique and the many penny-ante heists, computer crime remains essentially big business. A recent study by the Stanford Research Institute showed that in 64 percent of non-computer-related white-collar crime, the average take was \$100,000 per incident. In the period studied only 12 cases of computer-related embezzlement came to light, but the average take per "sting" was \$1 million.

With such rewards in prospect, computer crime seems destined to flourish, especially because the chances of detection are slim: discovery is more often by coincidence than by internal safeguards.

Many computer-crime cases are never openly reported because of the liability or the embarrassment that such disclosure might cause the victim. A large firm of private detectives was recently "stung" in a computerized payroll scheme that cost them an estimated \$50,000 per year. Rather than face public ridicule, the firm let the crime go unreported.

So, with the risks small and the rewards great, computer crime proliferates and the number of victims increases geometrically. The consumer, of course, pays for lost inventories with higher prices. The corporate executive who installs a computer system without adequate safeguards face personal liability for the loss of company assets. The investor relies to his detriment on financial reports reviewed by accountants who have not yet mastered the intricacies of computer-system auditing. The citizen suffers an invasion of his privacy when sensitive personal information is unwittingly disseminated to unauthorized "eavesdroppers."

The quantum jump in white-collar crime engendered by computerization results from certain basic facts about computer operations.

First, the computer is a faceless medium. There is a perverse challenge in "beating the machine." And such crime seems somehow less odious than face-to-face deceit. An element of gamesmanship is at work. The brief but absorbing chronicles of computer crime are full of stories about people who set out simply to prove that they could beat the system, and who only turned to serious crime after the rewards

of beating the system locked them into a life-style that they could not otherwise maintain.

Secondly, the sheer volume of data in a typical computer system "snows" the executive or auditor inspecting it. Computer printouts, endless rows and columns of numbers, themselves exert a hypnotic effect on the reviewer. Conventional theft is often hidden in a deluge of paperwork cunningly designed to muddy the mind of the auditor.

The alteration of electronic records leaves no erasures or telltale marks. It is done cleanly, and the operator needs only a split millisecond to "doctor" the entry and cover his tracks.

Computerization "brings all the eggs together in one basket." A single reel of magnetic tape may contain as much information as does a room full of filing cabinets. With thousands of accounts in process simultaneously, nickel-dime discrepancies in individual accounts can pyramid into formidable sums.

This leverage makes certain crimes, hitherto impractical, now eminently feasible. A few years ago, a major New York bank was victimized by a programmed swindle involving "breakage." "Breakage" is banker's jargon for the odd fraction of a penny or a dollar that is frequently not credited in interest calculations. The thief added the odd amount to his own account and altered the bottom-line aggregate records to cover the discrepancy. And the money rolled in!

This type of theft is particularly hard to detect. An auditing check "around the computer" would reveal only that the correct total interest was paid. Because the individual discrepancies are slight, the individual customer would probably not notice the difference; and if he did, he probably would not pursue the matter vigorously. These frauds are generally discovered only accidentally when a system fails or a change in systems forces manual processing or when parallel processing is performed to check out a newly installed system.

Although computers are often erroneously personified, the fact is that they can be programmed to assume quasi-human characteristics. Computer sleuths call this the "Trojan Horse" caper. A clever programmer can introduce a fraudulent scheme into the memory of the computer, where it can lie hidden and dormant, perhaps for months, then spring into action, set in motion by some external event.

In some cases this "Trojan Horse" concept has been taken one step farther. A *second* dormant program is injected simultaneously into the system. After the crime is a *fait accompli*, the second program will erase the first and cover its tracks. When the auditors arrive, they have no idea what happened. At first blush it may look as if the computer was the culprit, but actually it was just a clever accomplice.

The single most important inducement to the criminal has been the development of the new generation of "on-line" computer systems. In the on-line system the central computer that stores and processes data is connected directly to remote terminals; information can be introduced and retrieved at any one of the terminal outlets.

The central computer is connected to its satellite terminals by telephone lines, which generally run outside the computer users' physical control. The communication line can be bugged by inserting a variety of eavesdropping devices along the circuit; or, as in the Pacific Telephone case, assets can be stolen by mimicking or "spoofing" a legitimate terminal.

The spoofer can actively massage the system until the computer coughs up certain information or performs desired tasks. One tactic, called piggy-backing, is a hybrid between eavesdropping and spoofing. The piggybacker taps the target computer's communication lines, intercepts legitimate messages, and—using his own computer—modifies them for his own purposes. For example, in a bank-to-bank transmission, the piggybacker might insert additional credits to his own account.

The gullibility of computer users contributes to the vulnerability of on-line systems. Many users erroneously believe that digital communication is more secure than voice communication and that intrusion involves expensive equipment and sophisticated expertise. These users overlook, however, the widespread standardization that government regulations, international agreements, and the need for interchangeable equipment have brought to the communications industry. Furthermore, the industry's public-utility status requires that a great bulk of operational data be published and made readily available to the public.

Similarly, in the computer industry standard operating programs, common data transmission codes, and interchangeable equipment are basic ingredients of national time-sharing and on-line computer networks. This standardization greatly simplifies the development of compatible eavesdropping equipment of broad applicability.

The failure of computer users to appreciate the vulnerability of their systems is rooted in the "black box mystique" of the computer, which lulls us into a false sense of security and invites abuse.

The *User's Guide to Corporate Fraud* offered the following capsulization of prevailing misconceptions:

Computers were created by geniuses; therefore, they themselves are geniuses.

Computers generate tidy reports; therefore, they are correct.

Computers are supposed to save labor costs; therefore, they are cheap.

Computers can be programmed to answer any question decisively; therefore, they answer correctly.

The EDP (Electronic Data Processing) manager earns twice as much as the chief accountant; therefore, he must be twice as smart.

The FBI has drawn a bead on the computer mystique. In a few weeks the FBI will acquire its own third-generation computer system to be used as part of an expanded in-service training program aimed at combating the computer criminal. Special agent John Ryan, who directs the computer-fraud program at the Bureau's Quantico, Va., training center, explains:

We can't expect to develop sophisticated computer expertise in a four-week training session, but we can give each agent a basic familiarity that will dispel the computer mystique that has retarded law-enforcement efforts in the past.

Initially, we will focus on basic computer language and programming techniques; each agent will be responsible for writing and running his own programs. Later, the case method will be used to sharpen the agent's investigative skills. Our training computers will be programmed to duplicate actual computer frauds that have been perpetrated, and the agents will have to solve the "crime."

It is extremely important that the agent be able to identify exactly how the computer fraud was accomplished so that proper safeguards can be built into the system. . . . Also . . . computer expertise is often needed to preserve the evi-

dence necessary for conviction. Often such evidence is buried in the computer memory and special programs must be developed to retrieve the data.

The new head of the Justice Department's Criminal Division, Assistant Attorney Gen. Richard L. Thornburgh, intends to deal with computer fraud as part of a broad-based attack on white-collar crime. Thornburgh, the former U.S. attorney in Pittsburgh who earned his reputation successfully prosecuting a host of government officials, including a Pennsylvania Cabinet member and a state senator, responds, "As crime becomes more sophisticated, the response of law enforcement must increase in sophistication also. We hope that the FBI's program is a step in that direction. But we must remember that computer crime is simply one dimension of the white-collar crime problem which, if unchecked, will interject a hypocrisy into our justice system that breeds contempt and cannot be tolerated."

The Justice Department's computer-fraud efforts have their limitations. First, many computer capers occur outside the federal jurisdiction, and local and state law-enforcement agencies have been slow to fill the void. Second, all law-enforcement agencies are put in the position of reacting to computer crime. Only the computer user is in the position to take preventive measures.

All too often in the past, users purchased computer systems without a clear understanding of the computer's capabilities, from over-eager salesmen who emphasized a system's capacity for good work and not its vulnerability to misdeeds. Then, management delegated the installation, operation, and supervision to its data-processing staff, whose principle motivation was getting the most out of the system in order to justify its existence.

Should users reverse this scenario of benign neglect and recognize their responsibility, they will find no shortage of advice on proper security steps. After serving 40 days in jail for his Pacific Bell caper, Jerry Schneider set up his own security firm to advise clients how Jerry Schneiders could be stopped. For those who do not subscribe to the motto that "it takes a thief," one of the most comprehensive treatments of computer security is a handbook for businessmen entitled *The User's Guide to Computer Fraud*, edited by two computer sleuths, Stephen Leibholz and Louis Wilson, who were instrumental in developing the first commercial computers.

Misconception must give way to education. The Dartmouth College example must be replicated. At Dartmouth every student, regardless of his major, is required to take a basic course in computer technology. The business executive who played collegiate pranks with the computer will appreciate that culprits may be playing games with his firm's computer system. The educational efforts should also extend into our high schools—although this has backfired in at least one instance. A New Jersey computer firm donated several computer terminals to a local high school only to discover that a student used the terminal to break its own system's security code—instructing the computer to print out the message that became his calling card: "F—— you, the Phantom." This danger, however, is more than offset by the advantages that will flow from giving more citizens a clearer understanding of the computer's capabilities and limitations.

Unless we separate fact from fiction and recognize the open invitation to fraud, that data systems present, the computer crime wave will continue.

J. Taylor DeWeese, a Philadelphia attorney, served as a member of the Federal Advisory Commission on Computers.

[From Harvard Business Review, July-August 1975]

EMBEZZLER'S GUIDE TO THE COMPUTER

(Brandt Allen)

Do not let it bother you that the only reports of embezzlement schemes you have heard about have ended in the thieves being caught. Do not be discouraged by the fact that the takes reported in the press are so small. The really big, successful embezzlement schemes are still out there working, and working well. Most of the people who have been caught owe their capture not to the lack of their computer skills but to bad luck and mismanagement. You can be smarter. The author of this quick guide provides you with a rich sampling of embezzlement schemes that will work, and does a good job of laying some old fears about the difficulties of taking your company for a ride. His message is to take heart, learn from others' mistakes, and be clever.

Mr. Allen is associate professor of business administration at the Colgate Darden Graduate School of Business Administration at the University of Virginia. He has written a number of articles concerning computer security and fraud. This is his third contribution to HBR, the last being "Time Sharing Takes Off," which appeared in the March-April 1969 issue.

With the assistance of an on-line computer system, a young graduate student stole about a million dollars' worth of inventory from a large utility in California. The student acquired knowledge of the system by posing as a magazine interviewer, retrieving computer manuals from wastebaskets, and phoning employees. Eventually he was able to accumulate enough data, including system instructions and practices, ordering and operating instructions, catalogs, passwords, and the like to gain access to the equipment order system.

With his knowledge of company procedures and his access to the on-line system used for part of the inventory control system, the student was able to place orders for equipment to the utility's central supply division. The equipment would then be shipped to various designated warehouses, where, at early hours in the morning, in a designated truck, he would pick it up, along with the bill of lading. He spread his thefts over a number of field locations so that no single loss would arouse suspicion, and sold the equipment through a company he had formed.

By entering fraudulent data into the bank's computer from a remote terminal in his branch office, a chief teller of a major New York savings bank stole a million and a half dollars from hundreds of accounts. When quarterly interest was due, he would simply either redeposit some of the money or indicate that it had been redeposited. The manual auditing and the computer controls failed to show any fraudulent manipulation. The teller was not detected until a police raid on a gambling operation revealed that he was betting up to \$30,000 a day on professional sports. Even then the teller had to explain his manipu-

lations to the bank executives for them to fully understand what he had done.

As you can see from these examples, embezzlement may be the best game in town; it certainly beats the market for yield and return, and it is probably less risky. In fact, it is estimated that embezzlers take two to three billion dollars a year in the United States. (Since many if not most embezzlers never go public, only a sixth of the winnings and related incidents ever get reported in the press.) If embezzlers are detected, their penalties are almost always small. They rarely go to jail. The young graduate student in California, for instance, spent less than a year in detention.

As businesses and other organizations have automated more and more of their accounting and record keeping, embezzlers have found themselves faced with the problems of mastering and profiting from the new technology. Fortunately, the prognosis is good. Virtually all of the traditional speculation opportunities of the past may be safely run through the computer, and a host of existing new schemes is possible as well.

To sweeten the pot, computer technology tends to confound auditors and managers to the extent that they are rarely in a position to detect or prevent computer-based embezzlement. For example, of the more than 50 case examples I have studied, fewer than half were first detected by auditors or internal controls. A great many of these cases involved very simple schemes that could have continued to be successful for much longer, or for indefinite periods of time, had the perpetrator been a little more clever.

This guide is written both for the accomplished embezzler who wishes to polish his skills with computer technology and for the novice who correctly sees this field as a ripe new opportunity. The schemes most likely to be successful will be discussed, along with explanations of just how the computer must be manipulated. Examples of once successful but recently detected cases will be presented. Finally, a list of common misconceptions and important truths about computer fraud will be outlined. This is important since you, a would-be embezzler, may often profit from others' misconceptions.

THE BEST-LAID PLANS

To steal from an organization, it does not really matter what industry you are in or whether you work for a profit-oriented, governmental, or not-for-profit group. It does help, however, if you are in a position of responsibility and are a "trusted" employee—the greater your responsibility, the better. Knowledge of basic accounting, record keeping, and financial statements is also necessary, though the same is not so of the computer. You are in the ideal position of not needing to know a lot about computer technology in order to beat it. The auditors and management must, however, know a great deal in order to catch you at it. The best embezzlement schemes have to be well executed to work, but the ideas are simple.

Disbursements fraud: 'A voucher is the next best thing to money'

Without a doubt, the best place to start is with the fraudulent disbursements game. This fraud has historically accounted for more embezzlement losses than all others. The approach is actually quite

simple: your company, bank, or organization is fooled into paying for goods and services that it did not receive or did not receive in full measure. Payment is made to your bogus company. Arranging to cash checks issued to your company is certainly no problem; fooling your employer into issuing those checks is a bit tougher. Here are five things to remember when you start:

1. Carefully examine the accounting and record-keeping systems of your company. This can be done by personal inspection, unobtrusive questioning, and often simply by reading policies and procedures manuals or computer system documentation.

2. Study the purchasing function. Most organizations use a "purchase order" or similar document to order merchandise. Determine: who has access to blank forms; who is authorized to approve them; where copies are stored once the order is prepared and sent (in companies with advanced computer systems, the "image" of the purchase order is kept in the computer and may be read by authorized personnel in various departments; in this case there may be no written copies of the order); how form numbers are controlled (if at all); and what procedures are used for partial receipt of goods, cancelled orders, changes to unfilled-outstanding orders, and for all unusual transactions. This last item is particularly important; because the controls for nonstandard procedures are often the weakest, you should concentrate your efforts there.

3. Study the procedures for receiving merchandise. Often someone at the warehouse or receiving terminal verifies that the shipment corresponds to what was ordered by comparing the shipment to a file of open purchase orders. You must determine what verification is made and with respects to which documents, and what notification of receipt of merchandise is prepared, to whom it is sent, and where all the copies are maintained.

4. Watch out for vouchers. At this point in a purchase transaction, organizations often initiate a voucher record or document that uses vendor, purchase order number, account code, amount, receipt of merchandise document number, and related information. Learn as much as you can about this process and about the vouchers and the voucher file, because a voucher is the next best thing to money.

5. Find out how invoices are processed. The invoice is matched against the voucher to ensure that the invoice is correct and that the merchandise has been received; normally, a check is then prepared. Generating an invoice is the least of your problems, of course, since it comes from your bogus company through the mails.

The key point of the purchase transaction is this: whenever an approved purchase order is matched with a receipt of merchandise and with an invoice from the vendor, a check will be issued. You must be in a position to alter or fabricate both a purchase order and a merchandise receipt. After that, it is a simple matter for you to see that the invoice is rendered.

Exactly how you arrange to falsify the two key documents or records is, of course, the difficult part. If you work in purchasing,

you can generally find some way of generating fraudulent purchase orders by forging names of legitimate buyers, altering otherwise proper orders, or cancelling an outstanding order and using that purchase order number and authorization to issue a fraudulent order to your bogus company. Your problem will be to generate the merchandise receipt or record. The easiest method is, of course, to collude with someone in the receiving terminal, but many other devices, short of collusion, may be used. Sometimes this is as simple as printing either packing slips for your bogus company or merchandise receipts (employer's), forging them, and sending them through the company mail to data processing or accounting.

It is often much easier to establish both the purchase order record and the merchandise receipt if you work in accounting or data processing. Sometimes it is as simple as punching a few cards and entering them as if they were legitimate into a batch of transactions. The danger of doing this in second-generation computer systems is that the computer files of open purchase orders and merchandise receipts would not correspond to the various duplicate files maintained elsewhere—a constant threat. More modern computer systems often lack duplicate files because “purchase orders” and “merchandise receipts” are entered into a centralized set of computer files through computer terminals or data-collection devices. Here's an example to get you thinking:

Over a six-year period, the chief accountant of a large fruit and vegetable shipping company embezzled more than a million dollars. While running the accounting work at a computer service bureau, he developed a model of the company on which he experimented with both real and fraudulent disbursement transactions. He determined which company accounts he could take large amounts of money from without being detected. He then charged these accounts with phony purchase orders and receipts from punched cards he had prepared. By increasing these expense and inventory accounts, the accountant made the difference between what was actually owed and the recorded amount payable to a dummy company he had established.

The embezzler must be aware that his scheme is not complete just because he has been able to close the purchase order/merchandise receipt/vendor/invoice circle, and his dummy company has received the check. He has left “footprints” that are a potential threat to him behind in the company records. One footprint is that some account was charged for merchandise or services not received. It may have been an inventory account, in which case the book inventory figure is higher than the actual physical inventory by the exact amount of the theft. When the count of the physical inventory is made, your speculation should be exposed. There are, of course, many steps you can take to minimize such occurrences; these four stand out:

1. Select inventory accounts with high activity and high value, accounts that are physically difficult to count, where security is a continuing problem, where responsibility is shared among many, and where a certain amount of loss is “expected.”

2. Do not “hit” any account too hard. Try to find out how much shortage will be tolerated in each account before someone triggers a thorough investigation. Remember that there are likely to be

other white collar thieves at work (as well as thieves without collars).

3. Select accounts supplied by many new and constantly changing vendors.

4. Be aware of managerial style. Some managers are detail oriented. They pour over the financial statements, analyze the operating variances, and scrutinize the purchases, prices, terms, and inventory levels. Other managers are just the opposite. When charging a fictitious purchase to an inventory account, pick on the latter.

Many of the same arguments also hold for charges to expense accounts. Pick accounts that are difficult to monitor—ones such as freight, taxes, employee benefits, indirect labor, supplies, services, and so on. Avoid charging to small departments, departments run by detail men, and basic accounts, such as fuel, that tend to be watched closely.

Remember that all your efforts must be conducted through an accounting system with a number of tests and controls, checks and balances, cash totals, and batch counts. Fortunately, most of these controls are documented in the computer system descriptions or are the major topic of conversation of the data control group. You can also test for them by occasionally rearranging proper transactions; when the "real" test occurs, "they" will just think it is an error.

Inventory: 'It is easier to convert goods to cash'

Do not ignore inventories as a possible source of revenue. In many cases, it is easier to convert goods to cash than it is fraudulent checks, especially since the former are harder to trace. Although smaller, homogeneous articles might be easier to steal, size should not be a primary consideration, as the following example at an East Coast railroad suggests:

One or more employees in a railroad's computer center allegedly altered input data to aid in the theft of over 200 boxcars. It is thought that the rolling stock inventory file was altered to reflect that the cars were either scrapped or wrecked when they were actually shipped to another company's yard and repainted. The U.S. attorney handling the case stated that the actual thefts could not have gone undetected without the collusion of someone who had access to and was able to manipulate the railroad's computer records. If they can take 200 boxcars—just think what you can do!

Computerized inventory systems lend themselves to penetration for two basic reasons: they account for a large amount of material, and the controls on access systems are normally lax. Depending on the company and the location of its warehouses, inventory transfers or shipments are either recorded on supporting documents first and later key-punched and entered into the computer, or they are entered directly into a central system via computer terminals. Both systems are vulnerable to theft. (By this time you have probably noticed that I use the terms *fraud*, *theft*, and *embezzlement* interchangeably. See the ruled insert at end of article for more complete descriptions of the terms, and some idea of the penalties connected with the crimes.)

The computer can assist you because it lessens the visibility of your acts and may make it easier for you to gain access to the inventory files. Also, as in the example described at the beginning of this article,

interwarehouse transfers are often subject to less control because no one outside the company is usually involved in the transaction.

One day soon you will read about the following now-hypothetical inventory fraud:

A large manufacturing/wholesale company operating through a number of geographically separated warehouses linked by computer-communications to a centralized order-processing system found that several of its warehouses had been virtually "cleaned out." Apparently a computer other than that of the corporation was connected to the system and used to send shipping instructions to the warehouses. Because the company had relied on its central computer to keep records of all shipping instructions, there were no extra copies other than the bill of lading and the mailing labels, which were printed at the warehouse. As a result, there was no record of where the goods had been shipped.

Sales manipulation: 'Shipping documents are vulnerable'

Another fruitful area for the embezzler is the manipulation of shipments, sales, and billing procedures. Your objective here is to confuse your company into:

- shipping a product to a customer without sending the bill,
- shipping one thing and billing the customer for something else.
- billing a shipment at the wrong price.
- granting improper credits or adjustments on returned or damaged products.
- manipulating the sales commissions, allowances, and discounts on merchandise shipped.

For homework, prepare a flow chart of sales-order processing. Determine how all sales orders are received, written up, logged, and checked; how logs or registers are prepared, verified, and checked; and how sales commissions are processed. Study the flow of sales orders to the warehouse or plant and observe how orders are picked, packed, and shipped, and how all logs and registers are maintained there as well.

From your research you should have little difficulty in determining how to place an order (through a dummy company or one controlled by an accomplice). Your key task will be to intercept the shipping document or processed sales-order statement after shipment but before it is processed by the accounting department. For example, in many warehouses one can simply destroy a processed sales order after the order has been shipped. A helpful hint: most of the checking, logging, and registering controls you will have to beat were set up to ensure that the customer receives his order, not to ensure that your company bills correctly. Shipping documents are vulnerable to manipulation all the way from the warehouse to the accounting records in the computer.

In many computerized order-entry systems, the sales-order record is maintained on a computer file and is not normally updated or maintained until the order is shipped. When word is received that the order has been shipped, the sales-order record becomes the primary source of data on the shipment to accounts receivable and billing. The weak point in these systems is that the sales-order record can be changed after the shipment has been made but before the billing

processes are triggered. The time delay here may be hours or just seconds, but in all systems there is still a point of vulnerability. For example:

A middle-level manager in one large manufacturing company had access to the company's on-line order-entry, billing, and shipping systems. He was able to place bogus orders, which initiated the shipping of merchandise to a cover address. Then he would initiate billing cancellations due to alleged loss, damage, or destruction of the shipment in transit.

As I have noted, some companies have such weak controls that you can simply destroy the sales-order record after shipment and it will not be detected. In most cases, however, a register of sales orders filled is maintained, and a missing record would be noted. In this case, you may have to destroy the document after it has been checked against the log, or you might alter the record so that the eventual bill is much lower than what it ought to be. For example:

In a large Canadian department store, a systems analyst, using his knowledge of the sales-order processing system, was able to place orders for expensive appliances and have them coded as "special pricing orders." He was then able to intercept these orders in data processing and change the price to only a few dollars. When the appliances were delivered, he paid his account and closed the loop.

In most cases it is best to stick to only a few items per order and to order only items you know are in stock. In some cases, however, where a company's control over back orders and partial shipments is weak or nonexistent, just the reverse is true.

Payroll fraud: 'It is easiest in companies with a large, varying work force'

If you apply yourself, the payroll processing function in most large organizations with computerized control systems is a ready source of funds. There are a number of ways to manipulate your organization's payroll, but probably the most popular are:

- padding the payroll with nonexistent employees.
- leaving former employees on the payroll after termination.

Once you understand the payroll process thoroughly, you are ready to start. Employees in data processing, payroll, and programming are in ideal positions for these schemes. Perhaps the simplest method is to pad the payroll with extra hours, for oneself or for others as well, by altering input data; this does not require forging time records, or any other details. For example:

Over a five-month period a computer center employee who had both input and monitoring duties initiated checks payable to herself. Although she regularly deleted the check from the disk record, a surprise audit revealed that overpayments had been made, and she was discovered.

Such payroll schemes are, however, limited as to the amount it is possible to take, and involve more and more risks as the number of people involved increases. These schemes are also the ones payroll managers fear the most, and thus the ones they know how to control the best. As a result, unless controls are extremely lax, these schemes should be avoided. There are better ways.

Data-processing employees are often in the best position to create fictitious personnel, which is usually easiest to do in companies with lax controls and a large, varying work force. Supervisors of large departments often have neither the time nor the desire to verify the existence of each individual listed on the periodic check register (which they may or may not receive). In addition, the personnel department's employee data files are usually maintained in the EDP department and are subject to similar manipulation so that both files can be made to reflect the same fictitious employees. For example:

An employee in the data center at the welfare department of a large city entered fraudulent data into the payroll system and stole \$2.75 million over a nine-month period. He and several of his friends created a fictitious work force identified by fake social security numbers that were processed weekly through the payroll routine. The computer would automatically print a check for each fake employee, then the conspirators would intercept the checks, endorse them, and cash them. The conspirators were uncovered when a policeman discovered a batch of over a hundred of the fraudulent checks in an overdue rental car he found illegally parked.

In those companies that have numerous branches employing a varying number of employees, like opportunities exist. A branch manager can easily submit to the central processing group fraudulent information on temporary employees he has "put on the payroll." When the periodic checks are delivered, all he has to do is pocket those for the fictitious members of his work force.

Programmers who have complete understanding of payroll system controls and auditing methods have many, and often much more subtle methods that they can employ. A payroll program may be written to take a few pennies from each person's check and add them to that of the programmer. A better approach is to use the same scheme with income tax withholdings. The programs should, however, be designed so that the fraud segments can be activated or deactivated at will.

Pension benefits and annuities: 'Keep a deceased pensioner on the file'

You can often embezzle from funds destined for the payment of pensions, employment benefits, and annuities. While insurance companies and pension funds are the most fertile grounds for such frauds, a surprising number of other organizations also handle pensions, even if only on a small scale. Many businesses have small groups of special employees who, for one reason or another, have pension and benefit programs that are administered directly by the company rather than being taken care of through a pension fund.

The actual steps to be taken will vary depending on the size of the company and the extent and type of the pension and benefit programs. Regardless, you will first need to become familiar with the details of the operation to be embezzled: the numbers and list of beneficiaries, how beneficiaries are validated and revalidated, how benefits are determined, the addresses changed, and so on.

One of the most elegant frauds in the pension area—one that can run undetected for a considerable period of time—involves changing the address of a legitimate beneficiary to that of the embezzler or an accomplice at the time of the beneficiary's death. It is best to select

beneficiaries with no life insurance. Also, since particular attention should be paid to how death notifications are received and processed, employees of the computer center are often in the best position to operate this embezzlement. For example:

In a West Germany company, an employee operating a pension fraud left the deceased recipients' records in the computer system files but changed their bank account numbers, to which the checks were paid, to his own. When the pensioners were required to verify their existence, auditors uncovered the scheme.

If you are to be successful here, you must keep a deceased pensioner on the file only for a limited time, and then "kill" him.

If an estate does not claim death benefits after a beneficiary dies, you can claim them yourself through an accomplice. Again, personnel in the data center are often in the best position to know the status of each account, the requirements for processing claims, and if there has been communication between the company and the estate.

Rather than claim death benefits, it may be possible for you to claim the annuity or retirement benefits of a former employee who, for whatever reason has not applied for his legitimate benefits after a period of time. To protect yourself, you can make private inquiries as to why the person has not applied and, if the risk is low, proceed to claim them yourself.

Accounts receivable: 'The computer can be your scapegoat'

Theft from accounts receivable "robs Peter to pay Paul" by making good on one account with payments diverted from another. Popular long before the advent of computer systems, this "lapping" method does not necessarily require access to cash, though it does require constant vigilance; the amounts involved can mount up. The computer improves on the old scheme in several ways: in most cases, access to computer records is easier than to old manual records; your actions have less exposure when committed through a computer system; and the computer accepts all input as truth. Should a customer become suspicious because of repeated billings of a previously paid bill, a computer foul-up can be your scapegoat.

To succeed in this fraud, your main concern will be to shuffle the accounts continually. In addition to the accounts receivable section, ideal positions from which to operate this scheme are in the keypunch, data control, or computer operations departments. For example:

Two men diverted over \$61,000 in bill payments sent by insurance companies to a university medical center and deposited them in dummy accounts they had established. To cover their scheme, which lasted for ten months, the men deleted accounts from the medical center's computer records by making them uncollectible, or by purging them from the files. This fraud, like so many others, was uncovered by accident. One account was mistakenly left in the system, causing a second bill to be sent to an insurance company. A complaint followed which led to the discovery of the culprits.

If you install what is commonly called a program "patch" into a computer program, you can alter the program so that thefts can be more permanent. To accomplish this, you will need a good working

knowledge of computer programming, to know how to alter a program, and access to the program library.

It may also be necessary to "pass inspection" by the internal audit group, but this is not as difficult as it might appear since, as a practical matter, computer programs can only be tested by checking the results of test data. This method of inspection can ensure only that the program "does what it's supposed to do" not that it "doesn't do anything else" under unusual conditions, such as perform a different task when a particular switch is set "improperly" at the machine console, or when "unusual" transactions appear. In the trade, these are called "triggers."

An "unusual" transaction might be a debit and a credit of the same amount on the same day where the amounts are equal to the numeric data, e.g., a debit and a credit of \$112.75 on January 12, 1975 (10-12-75) might trigger a secret patch. The best trigger is one that, like the "unusual transaction," can be controlled from outside the organization. In theory, a complete test procedure should detect such tricks, but there is no guarantee; the internal auditor is always playing catch-up ball against you. Here is a good example of a patch.

A bank programmer patched a program in such a fashion it added ten cents to every service charge less than ten dollars and one dollar to those greater than ten. The excess charges were credited to the last account, which he had opened himself, under the name of Zzwicke. He was able to withdraw several hundred dollars each month until the bank, under a new marketing campaign, tried to honor the first and last names on their customer list, and discovered that M. Zzwicke did not exist.

Since they have the potential to enable the thief to prove that two plus two equals five, program patches, in spite of their difficulty and complexity, may be the embezzlement technique of the future. Companies have developed extensive controls over the processing of input data, in both receivable and payable accounts, primarily to detect and correct errors, but secondarily to prevent fraud. The "books" are assumed to be in balance at the beginning of the day, and if the day's transactions are clean and balanced, the ending totals are assumed to be correct and in balance. Thus the focal point of the controls is on the processing of inputs.

Using a program patch to cover fraudulent increases or decreases in balance can be especially profitable in large banks. The computer can be made to perform the old "adding machine trick" of the manual bookkeeping days in which bookkeepers totaling a series of ledger accounts could cover up a theft by advancing the tape, adding the stolen amount, and then repositioning the tape before finally punching the total key to get a desired but erroneous "balance." The computer program can also be made to "add" to the "correct amount" although not correctly.

A LITTLE LEARNING IS A DANGEROUS THING

There has been a paucity of published material about computer-related fraud, and because of this there are perhaps too many misconceptions about just how difficult it is to carry off. For some time, embezzlement has been the social disease of corporations, and they go

to great pains to avoid any publicity when incidents occur. As a result, there is only skimpy knowledge on how to do it successfully. Perhaps some of the following truths and fictions will help you.

Fiction: It's best to stick to banks

A number of computer frauds and embezzlements have indeed been detected in banks, insurance companies, brokerage houses, and other financial institutions. In fact, perhaps the first detected case of computer fraud was in a Minneapolis bank in 1966.

Embezzlement in financial institutions has received more publicity, probably because these organizations are, in many cases, regulated and investigated by federal agencies. But computer fraud has not been limited to financial institutions. There have been a number of examples of detected, computer-related frauds in manufacturing companies, wholesalers, utilities, chemical processors, railroads, mail order houses, department stores, hospitals, and government agencies. Given the reluctance of corporations and other organizations to publicize their own problems with embezzlement, these case histories, at the least, are examples of detected fraud in organizations that were unable to prevent publicity. However, it is evident, even from this small sample, that computer embezzlement works in places other than financial institutions.

Truth: Any organization can be a target

Fortunately for you, many executives believe just the opposite; they think embezzlement is something that happens to the other guy. This is, of course, the classic rationalization, and is the reason that general security in many organizations is poor. The potential for embezzlement varies with the type of firm, size, extent of controls, degree of audit, capability of the management and auditing personnel, as well as a host of other factors that are often unique to the organization. But there is probably no business organization, government agency, foundation, or not-for-profit organization that cannot be a successful embezzlement target. (Furthermore, the executive who says it cannot happen to him always makes the best patsy.)

Fiction: You need access to cash

Probably the most strongly held and most dangerous misconception executives hold is that the successful embezzler has access to cash or cash equivalent items, such as securities, in his day-to-day activities. Do not believe it. Many of the most exciting and lucrative embezzlements have been conducted by individuals who had absolutely no access to cash. Of all of the embezzlement schemes in this guide, only one involved people who had access to the "real thing." In fact, as most organizations have better control over cash and the people who handle it than any other part of their accounting system, there is a greater chance of embezzling funds if you do not have access to cash in your job assignment.

Truth: Collusion is beautiful

Corporations act as if there were some unwritten law of business that holds them responsible for embezzlement losses incurred by single individuals, but leaves them blameless if such losses are due to collusion. This is, of course, a ridiculous but nevertheless advantageous be-

lie for the embezzler. Furthermore, if you are willing to take the added risk, collusion can mean a many-fold increase in the take.

A good place where collusion works well is in banks. Employees in positions to make noncash, uncleared deposits appear as if they had been cash can and do bilk banks of thousands of dollars a year. With help, those thousands can become millions. There is nothing that a wise controller fears more than collusion between key individuals, and with good reason. For example:

Five men, including a vice president of one big New York bank and a branch manager of another, stole \$900,000 by running a float fraud between the two banks for four years. Deposit records were altered in the banks' data-processing centers so as to appear as cash deposits; the men would then withdraw cash. The fraud was detected only after a bank messenger failed to deliver some checks for a fraudulent "cash" deposit, and they overdrew one of their accounts by \$440,000. Otherwise the scheme could have continued indefinitely.

Fiction: Small and poorly managed companies are the best

It is true that small companies are not able to maintain the degree of internal control and separation of job responsibility and job assignments that a larger one can handle. It is also true that the internal controls and financial-system designs of poorly managed companies are more easily exploited than are those of well-managed ones. However, it is certainly a misconception that computer frauds have taken place only in small, poorly managed organizations. Some of the largest losses have occurred in the large companies. Furthermore, big companies are less apt to become suspicious of large losses than smaller companies are.

Truth: Look for special circumstances

One good rule of thumb is to always be on the watch for special circumstances that create opportunities for fraud, such as when a company converts from manual processing to a computer system or switches from one system to another. At these times unusual activities are less noticeable, and improper transactions and manipulations can be covered up. Exactly what you do is dependent upon what changes are being made and what position you occupy at the time.

Fiction: The old schemes will not work any more

Many age-old embezzlement schemes work just as well today as they did before computers were commonplace; many are even more successful because the computer makes transaction processing more predictable and reliable. Theft from dormant bank accounts is a good example. Long before computer systems were installed, bank embezzlers transferred money from accounts that showed very little activity to their own or to that of an accomplice. Today, the task is easier because more persons have access to the subsidiary ledger files, via the computer, and money can be transferred through a number of accounts at a faster rate. This makes the embezzler's actions harder to trace. For example:

A computer systems vice president and a senior computer operator of a New Jersey bank, along with three nonemployees,

stole \$128,000 from little used savings accounts by transferring the funds to newly opened accounts. The actions were uncovered when the bank switched to a new computer, disallowing the culprits a chance to erase their withdrawals as had been planned.

Truth: Some schemes are never detected

By definition, the only schemes known of are the detected ones. Considering the fact that a great many schemes are uncovered by chance, there must be a large pool of undetected embezzlement operations. For example:

A large bank in New York recently suffered a severe setback in trading in foreign currencies. That loss, together with certain other conditions within the bank, led to the suspension of dividends, a large run on the deposits of the bank, and eventual collapse. In the course of a full and complete examination of the bank, investigators discovered a large embezzlement scheme, unrelated to the losses on securities trading, that had escaped detection by the bank auditors and examiners. In the absence of the securities trading losses, this embezzlement scheme could have run undetected for a long period of time.

This and other accidental discoveries of embezzlement schemes lead one to believe that there is a great deal of embezzlement that goes undetected. In fact, *all* successful embezzlement is undetected.

A final word of encouragement: In just the few examples mentioned in this article, embezzlers stole over \$15 million with the computer's help. They were caught—but you can be smarter!

A 15-year-old schoolboy completely cracked the security system of a major London computer time-sharing service two months ago, gaining access to the most secret files stored on the computer by other users—able to read and change them at will without anyone noticing. He used no special technical gadgets and started with no special knowledge of the computers inner workings—instead he relied only on ingenuity and a teletype terminal in his school.

The schoolboy, Joe, is part of a new generation of “computer freaks” who explore computer systems in the same way that “phone phreaks” explored the telephone system. Joe worked on the project for only four months, until he was temporarily banned from the computer by his teacher.

Most users of the service have a terminal which is not permanently connected to the computer, and dial into it using the normal telephone system. After reaching the computer, the users must identify themselves by giving an account number and password. The trick Joe used was to listen to the sign-on procedure to learn the account name and password of highly privileged users, and then pretend to be them in order to gain access to secret files. . . .

He had the power to completely take over the system, cutting off other users, changing passwords, and even altering the bills that customers would have to pay. In fact, he never did anything much with his privileged account numbers. He wrote to the time-sharing service and told them what he did, but he never got a reply. A new version of the operating system was introduced on the computer early this month, and Joe said he planned to check it to see if his method still worked. .

KNOW WHAT YOU ARE DOING, OR LET THE PUNISHMENT FIT THE
CRIME!

If you are going to steal in style, it would be wise for you to understand the nature of your thefts, their legal classifications, and the statutes involved. Although the laws and statutes vary from state to state, the following are generally accepted descriptions of the illegal activities you will undertake:

1. Larceny is the theft of assets with the intent to convert them into cash without the consent of their lawful owner.
2. Embezzlement involves the theft of property by someone to whom the property has been entrusted (i.e., "larceny after trust").
3. Collusion occurs when more than one person is involved in cooperation for a fraudulent purpose.
4. Fraud involves the intentional misrepresentation of the truth to deceive the owner. In computer crimes the fraud occurs (a) when a thief attempts to conceal his actions through incorrect entries or changes in the company's records or files, and (b) when he is not entrusted with the assets that he actually steals. Most computer crimes fall into the fraud category.

If you simply steal inventory, it is theft, and if detected you may be charged with larceny. If you are an employee who steals and you disguise the theft, as was allegedly done at the railroad, that is fraud. If, however, you are the individual charged with responsibility for the inventory, your fraud is an embezzlement. If there is more than one of you, your embezzlement is collusion. For some delightful reason having to do with blue collars and white collars, thieves go to jail when caught, but embezzlers generally do not.

In a large percentage of cases, embezzlers are not even prosecuted. Because embezzlement is a crime against an entity and not an individual, a concept dating back to English common law, the criminal is often absolved if he or she simply returns the money. Also, because embezzlers are in positions of trust, they are often high up in the organization and friends of the top management, if they are not top managers themselves. Organizations naturally preferring to hang their dirty laundry inside settle such matters between friends.

[From Fortune, July 1974]

WAITING FOR THE GREAT COMPUTER RIP-OFF

(By Tom Alexander)

One morning last September, a computer operator on duty at Honeywell Information Systems Inc. in Phoenix was startled to see the output printer on his console start up all by itself. Out rattled a message referring derisively to a recent Honeywell press release about the company's vaunted new computer system, called "Multics." When it was done sniping at Multics, the mysterious message signed off with the words "ZARF is with you again."

ZARF is the code designation for part of a joint project of the U.S. Air Force and MITRE Corp., a defense-research outfit. The

project is concerned with computer security, and a favorite pastime of people involved in it is cracking "uncrackable" computers. The day before the Honeywell computer acted up, two ZARF men, Air Force Major Roger Schell and Steven Lipner of MITRE, visited Honeywell to look over the security features of prospective systems for classified Air Force computing chores. After seeing the press release about Multics, Lipner quietly placed a long-distance call to a ZARF colleague, Lieutenant Paul Karger, in Massachusetts, nearly 3,000 miles away. Karger, in turn, sat down at his teletypewriter computer terminal, dialed into Honeywell's private Multics system, and typed in a few subtle instructions that subverted every one of the system's safeguards, giving Karger effective control.

The ZARF prank was particularly embarrassing because Multics is designed with security as an uppermost consideration. Of all large commercial computers on the market, Multics probably incorporates the most elaborate safeguards against unauthorized tampering.

A STIRRING OF FEAR

The kind of vulnerability indicated by ZARF's little joke is beginning to disturb the keepers of modern electronic-data-processing systems. Most EDP systems consist of one or more large, multipurpose computers and banks of stored data, usually accessible via telephone circuits from individual terminals such as the teletypewriter that Lieutenant Karger used. Until not long ago, computer manufacturers and users saw little reason to fear that an unscrupulous person at one terminal would be able to read, alter, or delete another user's data, or tamper with the intricate programs that manipulate this data.

But in the past year or two, even the manufacturers have more or less come to acknowledge that it is not really very difficult for someone with a lot of skill to do things like that, even with the most secure systems now in existence. According to one expert, indeed, it's about as difficult "as solving a hard Sunday crossword puzzle."

HOW TO MAKE A PRESIDENT BLANCH

Computers, of course, have come to be deeply and pervasively involved in basic functions of our society. Top executives might die off, factories blow up, foreign subsidiaries get nationalized, but if you really want to see a company president blanch, ask him what he would do if the magnetic tapes with his accounts receivable got erased.

Electronic and magnetic data have not only replaced manually kept books, but have also gone a long way toward replacing tangible assets, including money itself. Today's credit-card system, for example, is an offspring of computerization. In the words of Richard Mills, formerly a top computer expert at M.I.T., and now a vice president of First National City Bank, "The base form of an asset is no longer necessarily a 400-ounce gold bar; now assets are often simply magnetic wiggles on a disk."

But gold bars in vaults, notations in a ledger, or, for that matter, written reports from a corporate research project are immutable and immovable things compared to magnetic wiggles, which can be read, altered, or destroyed at the touch of a teletypewriter key. For crim-

inal purposes, funds can be fraudulently credited to an account, a bank balance can be programmed never to fail, or the record of ownership of very large sums can be changed.

This is not to say that computer crime is an overwhelming source of loss as yet. Robert Courtney, who is the man responsible for the safeguards that go into I.B.M. equipment—and who is therefore likely to be one of the first people called when something goes wrong—ranks computer-related losses into six categories, in decreasing order of importance. The largest category, accounting for around half of all losses, is simply errors and omissions by clerical and data-processing employees. Next in order is employee dishonesty. Then come losses of data and equipment in fires; sabotage by disgruntled employees; water damage (i.e., floods and sprinkler-system malfunctions); and finally, an “other” category that includes remote manipulation of the system by outsiders.

But there seem to be reasons to fear that criminal losses—whether the work of insiders or of outsiders—will grow much larger as time goes by. For one thing, Courtney has found that employee dishonesty has risen from fourth place to second since 1972, which may mean that it just takes time for dishonest people to learn how to take advantage of their opportunities.

THE VANISHING PAPER TRAIL

Outside of the world of EDP professionals, most of the present concern about the latent problem of computer security seems to have emerged since the widely publicized Equity Funding insurance swindle. While really more an instance of old-fashioned fraud than a feat of computer manipulation, the Equity Funding rip-off could hardly have reached the magnitude it did without the computer's adroitness in fooling auditors from four different accounting firms. The case pretty well demonstrated that conventional auditing practice is all but helpless when confronting deception involving computers. The auditors have lost their traditional “paper trail”—the detritus of indelibly inscribed orders, invoices, bills, and receipts than the men in the green eyeshades pore through on the track of irregularity.

The main group to benefit from the Equity Funding revelations has been the small but growing corps of specialists who claim to be able to write programs to make the computer do the auditing—that is, to perform various accounting cross-checks and to throw up a warning when certain suspicious transactions occur. This sort of auditing, however, like everything else that goes on inside a computer, is only as dependable as the computer itself. And unfortunately, computers can be programmed to lie or conceal as easily as they can be programmed for truth.

Inklings of the computer's special potential for fraudulent use began to surface in the 1960's. The earliest federal prosecution came in 1966 and involved a young programmer in a Minneapolis bank who instructed the computer to ignore all overdrafts from his account. In that case, discovery occurred when the computer failed one day and the bank had to go back to manual processing.

A \$30,000-A-DAY GAMBLER

One of the more disturbing aspects of computer crime, in fact, is that detection, when it occurs, usually occurs by accident. Early last year, New York police raided a bookie and learned that one of his best customers was a man who for weeks at a time had gambled \$30,000 a day. When detectives looked into the man's background, they discovered that he was a \$11,000-a-year teller at New York's Union Dime Savings Bank. It turned out that he had access to one of the bank's computer terminals. For more than three years, he had been using the device to milk hundreds of savings accounts, netting \$1.5 million.

Combining workaday larceny with computer skill, he would accept a customer's deposits at the teller window and pocket most of the money. Later, he would go to a terminal and type in false information to the machine or instructions to transfer money into the customer's account from one of hundreds of accounts that had shown little activity over several years.

Cases like this involve comparatively elementary manipulations of the computer toward narrow aims, fundamentally no different from what the ordinary dishonest bookkeeper might try to accomplish. Furthermore, they're the kind of thing that computer auditing should be able to prevent. In the last couple of years, however, it has come to be recognized that the newer generations of computers, by the nature of their design, are vulnerable to more cunning forms of subversion.

THE "NONHOSTILE" ASSUMPTION

The leading expert on the history of computer crime is Donn Parker, a lanky former computer manager and now a researcher at Stanford Research Institute. Parker points out that "computer technology, over the years, was based upon the assumption of a benign, nonhostile environment." The machines were designed to provide maximum efficiency and convenience of operation by friendly, honest employees, within secure computer rooms to which access was limited.

In addition, the "third-generation" computers were put to uses not clearly anticipated by the designers. At the same time they were being developed, M.I.T. and other institutions were perfecting the concept of "time-sharing," which makes it possible for many individuals in remote locations to use the same machine simultaneously via terminals and telephone lines. Time-sharing put immense computational power at the fingertips of users who might never have been able to afford a computer of their own. A subsequent innovation, called "networking," made it possible to link several dispersed computers and data banks together, so that widely separated installations could share data.

SLICING TIME THIN

In all such "multi-access" systems, each user has the impression that the entire computer is at his disposal. Actually, the machine may be serving many users at once, reading each user's typed commands, parceling out milliseconds of time, and entering and removing pieces of programs and data in and out of the arithmetic circuits and memory banks in rotation.

While it's doing all this, the system is supposed to keep every user's data separate from every other user's through a system of secret passwords or code numbers, together with "access controls" programmed into the system itself. Each person types in his number or password at the beginning of his session to identify himself as a legitimate user. The access controls then specify what data and programs he is authorized to use, and "tag" and keep track of his work as it moves through the stages of processing.

These housekeeping functions are controlled by an immensely complex collection of special supervisory programs, called the "operating system." The supervisory programs are permanently stored in the computer and are altogether distinct from the "applications programs," which are the instructions for carrying out special tasks, such as a payroll run, bank's daily accounting, or a scientific problem.

For all its central role in managing and safeguarding the resources in a multi-access computer, the typical operating system of today is pathetically exposed to tampering. For one thing, manufacturers and users have to be able to make changes in the system's programs and data contents, including the passwords or privileges granted to any user. For this reason, the manuals that come with each system contain a number of standard code words called "systems commands" that act as keys to unlock or bypass the access controls or safeguards.

In many systems, therefore, all that a would-be wrongdoer needs is to be familiar with the manufacturer's manuals, know the telephone number of the target installation, and have access to a terminal. Then he can dial in, identify himself somehow as a legitimate user, and type in commands that make the system reveal its passwords, the names of other users, their privileges, data files, etc. Once he has the passwords, any user can then masquerade as another user or as a staffer with authorization to make changes in the system's password-privilege list, or, for that matter, in the operating system's own programs.

THE PERILS OF COMPLEXITY

Like the passwords, the systems-command code words are arbitrarily chosen and can be changed as easily as the lock on a door. That would foil inexpert intruders, but crack programmers have demonstrated that it's not necessary to know the systems commands to take over any major operating system that now exists. For one thing, each of the command code words is really a shorthand symbol that stands for a prewritten miniprogram stored in the computer. When the word is used, this program carries out the various steps required to unlock the system's safeguards. A skilled would-be penetrator with access to the proper manuals can deduce everything he needs to write his own program, type it in, and subvert an operating system.

Another important kind of vulnerability derives from the sheer complexity of today's operating systems. To cope with all eventualities in a time-sharing network, some operating systems run to hundreds of thousands of separate instructions. In the composition of something like that, hundreds of errors inevitably creep in—either oversights in the design of the safeguards or simple mistakes in the

writing of the instructions. Many of these errors in concept or execution must be located and corrected before the system will work at all, but some remain hidden, or annoyingly evident, for years.

Under certain circumstances, these errors will let data leak from one user's domain to another's, or even open a way into the supposedly inviolate territory of the operating system itself. Many a subscriber to a commercial timesharing service, having accidentally pressed a certain combination of keys, has found someone else's data rattling out unbidden. By now, a lot of people have learned how to exploit software errors deliberately—not only to read data stored in the machine, but also to type in changes on access-control safeguards, data, and programs.

ATTACKS BY TIGER TEAMS

The first delighted exploiters of these software quirks were the "systems hackers"—students at universities where some of the first time-sharing systems were installed as far back as the middle sixties. Among other things, faculty members stored grades and examinations on some of these systems, and systems hackers became adept at changing their own grades or reading upcoming exam questions.

By the late Sixties, computer experts at Rand Corp. were warning their government patrons that all the multi-access systems on the market were vulnerable. Over the years since then, under contracts with the Defense Department, Rand and a number of other organizations have been seeking methods to improve operating-system security, as well as methods to ascertain whether any system is really secure. The most glamorous phase of this activity is the work of the "tiger teams," who actually try to penetrate systems being considered for defense uses. So far, no major system has withstood a dedicated attack by a tiger team.

The disturbing implications of all this for civilian computer operations are only now coming to be widely recognized. In principle, the ability to take over a computer's operating system implies having access to all data and all programs on the machine, together with the ability to distort them at will. Properly done, such subversion is likely to go undetected. For criminal purposes, such control would be something like having a small army of corrupt bookkeepers at one's command, but without all the risks of exposure that relying on the cooperation of human beings entails.

With the increasing use of these systems as repositories and conveyors of valuable assets and private and proprietary data of incalculable worth, a number of computer professionals have begun speculating about the grave potentialities for criminal manipulation of computer systems. Among them is Clark Weissman, a manager of computer-security research with System Development Corp. Weissman believes that a lot of criminal activity could already be going on, leaving no external evidence.

"Sherlock Holmes," he says, "can't come in and find any heel marks. There's no safe with its door blown off. Many companies wouldn't even know their data's been manipulated." As for auditing programs, "the first thing the interloper would do is corrupt the audit-trail software itself."

“THE COMPANIES JUST EAT ’EM”

No one has valid statistics as to how much of this sophisticated subversion goes on, but from all indications, a lot more goes on than is ever detected. Donn Parker concludes that of nearly 175 cases of computer crime he has looked into, hardly any were uncovered through normal security precautions and accounting controls—nearly all were exposed by happenstance. One expert guesses that the ratio of undiscovered to discovered crimes may be on the order of a hundred to one.

A lot of computer crime that *is* detected, moreover, is never publicly announced. Most security experts have collections of incidents that they have investigated but that were never reported to the police. Furthermore, some banks and companies candidly admit that when an incident is discovered, the corporate victims usually try to avoid the embarrassment and loss of confidence that publicity might bring. According to I.B.M.’s Robert Courtney, “It’s generally accepted in this business that about 85 percent of detected frauds are never brought to the attention of law-enforcement people. The companies just eat ’em. Of the 15 percent that are announced, a fair number are brought in from the outside by the police.”

What often happens is that the offender, once detected, is required to make restitution and then leave—sometimes even getting severance pay and letters of reference to speed him away. One consequence, no doubt, is a circulating population of unpunished, unrepentant, and unrecognized embezzlers going from company to company. Probably a more serious consequence, though, has been to suppress recognition of the extent of computer crime, and thereby to lull both makers and users of computers into minimizing it as a threat.

TEN THOUSAND DISHONEST PROGRAMMERS

Computers appear to have magnified the potential rewards to the criminal. Parker analyzed twelve cases of computerized bank embezzlement that occurred in 1971 and found that the losses averaged \$1.09 million apiece, or about ten times the average embezzlement loss. With ever larger amounts of credit and other assets moving onto EDP systems, it seems inevitable that more criminally inclined people with more elaborate resources will grab for the prizes so temptingly exposed. “There are something like a million programmers in the country right now,” observes Willis Ware, a pioneer computer-security expert at Rand, “and if only 1 percent of these were inclined to be dishonest, that’s ten thousand dishonest programmers.”

Especially troubling is the thought of even a 1 percent incidence of dishonesty among the “systems programmers” who write the operating systems for the computer vendors or modify them to fit the needs of particular users. These programmers are the people most knowledgeable about the intricacies and weaknesses of specific systems. Jokes Robert Jacobson, a vice president of Senator Security Group, Inc.: “Ideally, the first step in securing a system would be to shoot the programmer.”

In a really big job, the programmer or programmers would probably have accomplices with other skills. A somber prediction along

this line comes from Robert Abbott, director of an Advanced Research Projects Agency computer-security project at Lawrence Livermore Laboratory. "It's only a matter of time," he says, "until somebody mounts a team-directed approach, involving programmers, accountants, and maybe wiretappers and burglars. When it happens, it's going to be awful."

PASSWORDS IN WASTEBASKETS

One impediment to would-be perpetrators is the difficulty of obtaining detailed knowledge about a given organization's EDP system, procedures, and accounting controls. Aside from that problem, the principal defenses against computer frauds right now are the passwords. And passwords often turn out to be a laughably weak defense, even against those without fancy programming skills. A lackadaisical attitude toward security persists in many EDP installations. For instance, it's apparent to the casual visitor that he would have little trouble walking into the offices of the average time-sharing company or service bureau—posing perhaps as a prospective customer, a delivery messenger, or even a legitimate but confused user—and proceed to scoop up proprietary tapes, printouts, or passwords.

It has also been demonstrated on more than one occasion that a persuasive liar on a telephone can entice employees of a time-sharing system into giving out passwords. In all sorts of computer installations, people bandy passwords about or write them down. Wastebaskets galore are stuffed with printouts on which passwords are visible. And often there will be some employee who will provide passwords for a bribe.

Everything else failing, a prospective intruder has technical means at his disposal. For example, he might dial up a system, plug a small computer into the line, and set it to trying out passwords.

Generally speaking, computer security is obtained only at some cost, and among the costs is inconvenience to the ordinary human beings who must use the machines. Many organizations, in seeking a proper balance, often put convenience to their harried, forgetful users ahead of airtight security. In the case of commercial time-sharing services, at least, it appears that if customers are really concerned about the privacy of certain information, they'd better keep it out of those systems.

Other defenses besides passwords have been devised. One possibility is to program the computer to identify legitimate users by asking random questions about family background, etc. "The trouble with that," says I.B.M.'s Courtney, "is that if you're running thousands of transactions a day, you don't much care to spend ten seconds or so every time arguing with the computer about who you are." I.B.M. is currently trying out, among other things, the use of magnetically striped cards that users can insert into terminals to prove their identity. Already, though, tinkerers have found that it is no great feat to counterfeit such a card, using ordinary magnetic tape. A number of companies are working on devices that will recognize personal insignia such as the shape of a hand or the unique motions an individual makes as he signs his name.

A NEW KIND OF PIGGYBACKING

Even with elaborate passwords, magnetic identity cards, and other screening procedures, along with thoroughly honest employees and guarded computer rooms and terminals, most multi-access systems have a huge sector of vulnerability: the telephone lines that stretch from one facility to another. Experts contend that it is technically a simple matter to tap into phone lines and thereby learn passwords and identifying signals, transmit false data, or penetrate an operating system. One ingenious wiretapping tactic, called "piggybacking," involves hooking onto the tapped line another computer that intercepts legitimate messages and modifies them. A piggybacker could, for example, insert additional credit transfers to accounts during a bank-to-bank transmission.

About the only defense against wiretapping is some method of scrambling or encrypting messages. It happens that this is something a computer can do quite handily. It also happens, however, that computers are very handy at *breaking* encryption and scrambling schemes, often in a matter of minutes or hours. Staying ahead of a sophisticated tapper would take both elaborate encryption schemes and provisions for changing the keys to the encryption at frequent intervals. This would impose a considerable burden in hardware costs, together with the potential for chaos if keys get lost or mixed up.

THE CASE OF THE PHONY FOREMAN

While ignorance of the computer system and accounting controls will probably stop the casual intruder, it's not likely to deter for long the dishonest employee or the sophisticated and highly motivated thief. As Donn Parker puts it, "The most dangerous threat is the penetrator who knows as much about the system as you do."

Such was the case in one of the more ingenious computer crimes so far, the work of a baby-faced young Californian named Jerry Schneider. Around three years ago, at the age of nineteen, Schneider spent some months learning the necessary codes and procedures of the system that Pacific Telephone & Telegraph Co. used to handle field orders for communications equipment in Los Angeles. Among other things, he posed as a magazine reporter to gather the information. He also used his own computer terminal to probe the system.

Eventually Schneider learned enough to pose as a field-supply foreman and, using a pushbutton phone, tap in orders for equipment—phones, Teletypes, switchboards, etc.—to be delivered to field locations, including manholes. Then, with an old phone-company truck, Schneider or one of his employees would pick up the goods and sell them. Schneider used his entry into Pacific Telephone's computer to keep track of current inventory, and on occasion, after spotting shortages, he sold the company some of its own equipment.

One of his thirteen employees eventually turned him in after a wage dispute, but not until he had operated for nearly two years and stolen nearly a million dollars' worth of equipment. After serving forty days in jail, he went into the business of advising clients on how to prevent computer rip-offs. His motto: "It takes a computer thief . . ."

Computer manufacturers are trying hard to develop systems that will be more resistant to manipulation, by either dishonest employees or outsiders. The consensus of the experts seems to be that it is possible to design penetration-proof operating systems, but that they're not likely to be commercially available in large systems in less than four years, at the earliest. When they *are* available, the problem will then be what to do about the existing systems. According to International Data Corp., an authoritative industry source, something like \$17 billion has already been invested in remote-access computer hardware, and probably even more in software. Most of this stuff has ten years or more to go before the investment is amortized.

Right now, expert opinion is divided on the question of whether, even in principle, any of the existing systems can be rendered sufficiently secure to handle assets or information of very high value in the face of a sophisticated attack. Contends Steven Lipner, one of the perpetrators of that ZARF prank in Phoenix: "There are two difficulties with trying to retrofit one of these large monolithic operating systems to get better security. One, it's expensive, and two, it doesn't work."

IT MAY TAKE SHOCK

Others, however, believe that security can be significantly strengthened. As one measure, some advocate the use of separate mini-computers and software as gatekeepers, to handle the chores of user identification and access control. The main purpose is to remove these sensitive functions from the intricate maze of a main operating system.

While they are showing more and more interest in these new developments, the manufacturers contend that it's fairly pointless to bring out systems capable of resisting sophisticated attack until their customers adopt better physical security measures in their own installations, as well as better screening of computer employees. And while customer interest in the problem has picked up a lot since the Equity Funding scandal bubbled up, there's still reluctance to spend much money for computer security. It may take the shock of dramatically expensive and well-publicized computer crimes to start the money flowing in any abundance.

There's talk in the trade of numerous large rip-offs. One story tells of a young swindler who arrange false credit transfers into two major banks from two other banks within a span of two weeks, and escaped with nearly \$5 million. But no really big computer crimes, involving tens of millions or more, have surfaced in the public domain. A great many people in the computer-security business wonder aloud when that huge rip-off is going to happen—if it hasn't already, undetected.

[From Journal of Commerce, May 19, 1975]

INTEREST IN COMPUTER SECURITY MUSHROOMS

(By Lynn Brenner)

The many problems revealed by the Equity Funding scandal have acted as a boon to the small and growing industry of computer auditing security analysts, according to an expert in the field.

"Equity Funding has been a blessing to my business," Joseph J. Wasserman, president of Computer Audit Systems told *The Journal of Commerce*. Computer Audit Systems has run seminars on auditing techniques for several years, he said.

In the past, attendance has been about 30 people per session, but since the Equity Funding case revealed the immense vulnerability to fraud in computer systems, attendance has jumped to 55 people per session, and it is executives from insurance companies who represent the majority of the new attendees.

In the past, Mr. Wasserman said, many companies which had complex computer systems did not understand the importance of sophisticated security controls—in some cases, even simple practical precautions.

An audit control and security firm is selling an intangible, Mr. Wasserman said—but an extremely important one. He described the following vulnerabilities in a computer system: fraud, loss of information, delay of information, and human errors, as well as exposure to fire.

One of the largest areas of loss in the computer business, he said, springs from human error. Usually the mistake is made when information is not correctly input into the computer.

A computer which keeps track of frequency of billing, on insurance policy premiums, for instance, if not fed the correct code, will bill an insured on a yearly instead of the correct monthly basis, or vice versa.

The result is that insured are either under or overbilled. The most common type of computer fraud, Mr. Wasserman said, is one in which the input data is manipulated. False data fed into the computer will produce checks to pay phony invoices, for instance.

Another method is to alter the computer's programming code. In a banking environment, for instance, if the code is changed to compute interest to within a cent rather than to a tenth of a cent, a thief can accumulate quite a sum over a period of time.

Since the computer has been programmed correctly, the books will always balance. And by deleting the code afterwards, the criminal will have committed "a trackless crime," Mr. Wasserman said. "No one really knows how much of this kind of fraud exists," he said.

INFORMATION WORTH MONEY

Data banks also contain information which itself is worth money—policyholder names are worth something for mailing lists. A life insurance plan can be sold to another company.

A computer system which permits a time lag can also encourage dishonesty. Mr. Wasserman cited the case of one company which had five subsidiaries, each with its own computer.

Company policy was to have each subsidiary compute earnings accounts by the 3rd of each month, and forward them to company headquarters, where they were consolidated by top management by the 12th of the month.

Financial management first became aware that the time lag was causing a problem when a stock broker remarked to a company executive that many people in the subsidiaries seemed to have an uncanny early knowledge of when to buy and sell company stock.

No one really knows how many undetected computer frauds there are, Mr. Wasserman said. And there are no standards to go by, in applying security measures, because the field is so new. The standards are being created on the job.

SELLS NO SECURITY DEVICES

Computer Audit Systems does not sell any security devices, he pointed out, and thus is able to give objective advice. The effort, he said, is to give practical, workable advice, which is tailored to meet the individual customer's needs. Many common problems can be corrected at little or no cost.

Among the most common deficiencies are inadequate fire safety measures. Computer rooms have "floating floors," Mr. Wasserman explained, floors which leave room underneath for cables. The flooring can be lifted with a suction cup floor puller. In one company, Mr. Wasserman said, when he asked for the flooring to be lifted so that he could check the cables underneath, employees could not find the floor puller anywhere. In the case of a fire, he pointed out, this kind of loss would be disastrous.

Computer rooms are also extremely vulnerable to paper fires, he pointed out, and an extremely common mistake is to equip such rooms with fire extinguishers which are too heavy and placed too high on the wall to be easily handled by computer operators. Extinguishers which contain CO₂, a gas, only feed a paper fire. Plastic trash cans, instead of metal ones, can spread a fire, besides producing noxious fumes and smoke which will damage electronic components.

USE OF FIRE EXTINGUISHER

Computer operators are also frequently unaware of how to use a fire extinguisher. "Just pointing and turning it on doesn't work," said Mr. Wasserman. "There's a pin you have to pull to release the extinguisher, and most employees don't know this. We advise clients to contact the local fire department and get training for their employees. It doesn't cost anything. The results are amazing—70 to 80 per cent of those trained go out and buy fire extinguishing equipment for their own homes."

Another important area frequently ignored is "back up"—the stored computer tapes which represent years' worth of records. Off-site storage of magnetic tapes is common, Mr. Wasserman said. Companies will frequently send tapes out to the vault when they are three days old, and think that in case of accident, their Master files will be up to date within three days.

But often those stored tapes cannot be run at all—if the computer has been changed, an old computer is needed to run them. Many companies don't think to retape all their files so they can be run on the new machines.

In one company, Mr. Wasserman said, random selections from a 30,000-tape library revealed that many of them were not runnable. Ten-year-old tape, unless it is high quality, deteriorates. Temperature controls are vital to the life of the tape, and only the best quality tape should be bought for archival purposes, Mr. Wasserman said. If per-

sonnel changes have occurred, there may be no one in the company familiar with the source program, the code which enables the old tapes to be run.

In one insurance company, Mr. Wasserman said, he had found that only one man, a company executive, was actually familiar with the computer program. He had risen in the company from the computer room and was still consulted for any computer program problem.

The computer program had never been documented, and no one else knew it. What if the executive left the company? What if he died? Careful documentation is a vital security measure in any computer system, Mr. Wasserman said.

[From *Datamation*, January 1974]

THE NEW CRIMINAL

(By Donn B. Parker and Susan Nycum)

There are the same old crimes of fraud, theft, larceny, embezzlement, vandalism, and extortion. But many of the environments of crime and the people in those environments are changing. Computers are taking over sensitive functions in business and government where there has traditionally been great leverage for gain by unauthorized acts. The people who used to perform those functions—clerks, accountants, other financial workers, their managers—have been replaced by people in the new EDP occupations; their work has changed to monitoring and using the processes now done by computers.

We are obsoleting many of the traditional white-collar criminals and some of the professional criminals. They no longer have the skills, knowledge, and access to perpetrate their old crimes. The *Wall Street Journal* frequently reports criminal acts where two men drive up alongside an elderly messenger carrying several million dollars worth of negotiable securities from one firm to another on Wall Street. One man jumps out, hits the messenger over the head, grabs the securities, and escapes in the car. This will be an obsolete crime in a few years. Negotiable securities will be stored magnetically and electronically as data inside computers and transmitted over communication circuits from one computer to another. Perpetrators of securities thefts will need the skills, knowledge and access associated with computers and data communications technology; they will not be dealing with as simple a victim as an old messenger. If these crimes are going to continue to proliferate, they will have to be done by people in EDP or related occupations, and must involve computer and data communication systems.

CASE HISTORIES

Experience indicates a growing sector of crime and unauthorized activities within EDP and associated occupations. Some of the more significant personally verified cases are described below, but names of perpetrators and victims are withheld since their continued exposure serves no useful purpose. These are a few of the 160 recorded case histories collected at Stanford Research Institute in studies conducted over the past three years.

The first programmer convicted for stealing programs in a 1964 case received a five-year term in a Texas penitentiary. He stole copies of \$5 million worth of programs from his employer by saying he was taking them home to work on at night. This is the only computer-related crime thoroughly reviewed for law library reference purposes.

The first federal criminal case occurred in 1966 when a 21-year-old programmer put a patch in his program to ignore his own checking account in checking for overdrafts. He concluded that this was the easiest way to solve his small financial problem. It would cause the least amount of trouble to the least number of people. He figured that the discrepancy would not cause harm to the bank or the computer system for just three days, after which he planned to secretly make restitution and remove the patch. Three months later the patch was still in the program and he was \$1,300 overdrawn; the computer happened to break down and hand calculations revealed the discrepancy. He was convicted and received a suspended sentence. This was the first case in banking history where a nonemployee of a bank was ever convicted of altering bank records. He was employed by a facilities management company operating the computer for the bank. After being fired from his job, the same management company contracted for his services; good programmers were hard to find in those days.

An accountant was discovered in 1968 after six years of embezzling over one million dollars in a simple receivables/payables theft using dummy vendor companies with accounts in a local bank. Although the act had nothing to do with computers, he used a computer he ran in his own service bureau to simulate his employer's business to test his planned thefts (to make sure they would be dispersed and small enough to go unnoticed). He was caught when he stopped using the computer to decide limits of his theft rate. He received a full ten-year sentence because he was unrepentant and refused to tell what he did with the money. (Anyone who knows how much it costs to run a losing computer service bureau could guess where the money went.) He had become a time-sharing salesman by the time of his indictment and trial and told his customers he had another opportunity that he couldn't refuse just before he went to prison.

The first case of stealing a program from the memory of a computer over telephone circuits and a remote terminal in 1971 caused world-wide publicity, including three-inch headlines in the *Paris Herald Tribune*: "COMPUTER RAPED BY TELEPHONE." It was the first case in which a search warrant was issued to search the memory of a computer for evidence. A programmer was convicted and given a suspended sentence for theft of a trade secret even though a witness in a related civil suit revealed that it was common practice for programmers in both companies involved to gain unauthorized access to the other's computer.

One young programmer took all the programs of his employer, a small medical accounting firm, went to hide in the mountains and told his employer he wanted \$100,000 to return them. He was caught, but the prosecutor dropped the case. However, the programs were impounded for evidence, and the small company

burglarized the sheriff's office to make copies of them just to stay in business.

A "Trojan Horse" technique was used to compromise the security of a campus time-sharing computer system. A user submitted a utility program for general use. That program contained code to take over the operating system if it ever ran at the same privilege level as the supervisor. After several months, a computer operator used it, triggering the hidden logic and causing the operating system to read still another program into system resident memory, and erasing all trace of the illicit Trojan Horse code. The perpetrator could then gain complete control of the system at any time using a specified user code. The trick was discovered when a maintenance programmer found the strange program in a memory dump, and in dumping the files stored under the special user's code found the text of a complete confession and a description of the method. In a similar case, the Trojan Horse used to bring in illegal code was a program to print out a picture of Santa Claus, which elicited the comment, "Is nothing sacred?"

Additional recent cases include the \$1.5 million New York Union Dime Bank embezzlement, the \$2,000 million Equity Funding Insurance fraud, the \$1 million Los Angeles Telephone Company equipment theft, and the \$300,000 Long Island and Pittsburgh Westinghouse embezzlement.

THE VULNERABLE FACILITY

An analysis of the characteristics of these cases has provided a description of an imaginary computer facility most vulnerable to the new criminal. The weaknesses are described below in descending order of importance.

The computer system is used for financial processing applications including payroll, accounts payable and receivable, and storage and maintenance of files of financial data. The system puts out negotiable documents and takes in data representing negotiable documents. The system also stores and maintains other valuable data such as mailing lists and inventory of goods lists.

Among the employees, there is more mutual loyalty to each other than to the employer. The staff has more self-interest than interest in the success of the organization. Morale is low, and small groups join in defensiveness toward management and society. Employees reinforce one another in rationalizing acts that management would not condone.

The organization does not separate sensitive job functions and lacks dual control of important tasks. Most serious is the non-separation of application programming, program testing, systems programming, data input and output handling, customer servicing, materials storage, and computer operation. Separation is missing in tasks, responsibilities and physical access.

The system services and physical facilities are available to some employees during nonworking hours and without supervision. The absence of responsible staff in nonbusiness hours is not compensated for by sufficiently increased physical security.

Computer programs, including the operating system, are not under modification control, and ownership is not sufficiently displayed or otherwise established. Programs do not include sufficient controls, tolerance checking and anomaly testing. Exception reports produced during processing contain little information indicating unauthorized activity, but contain volumes of useless data that burden the auditor beyond his comprehension and attention span.

Disgruntled employees are not identified and removed from sensitive jobs. Employees being released from positions of trust are not immediately removed from their work areas and positions of system access. Use of computer facilities, materials and services is not monitored or sufficiently controlled.

A profile of the computer criminal, or at least some characteristics, is starting to emerge from these studies, which have included many hours of interviewing perpetrators. Some of the characteristics are consistent with findings about white-collar criminals in general, but still unknown to most people in the computer field.

Perpetrators are highly motivated, bright, energetic, and generally young—18 to 30 years old, except for a few of the embezzlers who are older. The few women found among perpetrators are usually keypunch operators or clerks. Perpetrators seem to easily obtain all the information they need about a system involved in their acts. For example, one thief posed as a magazine writer to obtain a detailed briefing about an equipment ordering system and get introduced to all the key people. He soon knew more about the system than anyone in the victim company and its penetration was simple. No computer facility exists today that a bright perpetrator couldn't penetrate if the reward were great enough. Many systems do provide significant rewards, as we know, because losses of \$100,000 to millions of dollars have been experienced in many of the recorded cases studied.

The elements of challenge and game-playing are significantly stronger among computer criminals than among other white-collar criminals. This is not an unexpected finding, considering the strength of these factors among computer technologists. In some cases, claims of victims that their computer systems were safe and could not be penetrated encouraged eager young programmers who look on their work as an intellectual challenge to pit their minds against the intransigent machine. University campuses commonly have their resident "system hackers" ready to accept any challenge of professed security in and around campus computers. However, these people usually become frustrated in their successes unless there is some way they can take credit publicly for their achievements. One perpetrator who claims to have gained over one million dollars from his deeds said that aside from making money rapidly, his motive was to see how far he could go with his crime before he stopped and informed his victim of his acts. He was confident that the victim could not find evidence of his act even if he confessed.

The "Robin Hood syndrome" is common. The young man described above indicated that doing harm to people is highly immoral; but, he said, government-regulated industry and telephone companies in particular do great harm to society so doing harm to such organiza-

tions is fair. This differentiation between doing harm to people and to organizations has some current popularity. The computer within the organization is an additionally attractive and satisfying target capable of sustaining loss, but not possessing emotional reaction that might produce feelings of guilt in the nonprofessional criminal. This is the "vending machine syndrome" experienced by most of us; it makes us unemotional, guiltless, coin-return thieves.

Often the perpetrators' acts differ in only small ways from the accepted or normal practices of their associates, such as the program theft by telephone described above. People within an edp organization can degenerate in their practices in many ways to levels allowing rationalizations that lead to serious criminal acts.

Even the "skyjack syndrome" (where the crime becomes "popular") can be observed in computer-related crime. The fraud technique of replacing blank deposit slips on bank counters with the perpetrator's own MICR-coded slips, knowing that the bank's system would assure a large increase in value of his account, was given great publicity when it occurred in New York City. The same technique was soon reported in Boston, Los Angeles, and Washington.

It appears that the perpetrators strongly fear unanticipated detection and exposure. This makes detection as a means of protection at least as important as deterrence and prevention. Perpetrators tend to be amateur, white-collar criminal types for whom exposure of activities would cause great embarrassment and loss of prestige among their peers, in contrast to many professional criminals who want their peers to know of their accomplishments.

The only means of locating potential perpetrators is to find those with the technical skills, knowledge, and access—the people in EDP and related occupations. A high rate of collusion has been found, since the computer-related crime methods often require skills, knowledge, and access possessed by more than any one person. This lends support to the value of separating responsibilities among EDP employees.

The increasingly sensitive nature of edp occupations in business and government organizations and the potential for doing harm should produce concern for the trustworthiness and ethics of EDP people. Almost every keynote speaker at national computer conferences for the past few years has alluded to this concern. The occupations have been populated with people moving from other occupations, with varying kinds and levels of ethical standards, resulting in confusion and ambivalence.

For example, a concept called the "Peninsula ethic" has grown out of the program-theft-by-telephone case cited earlier. A well-known computing consultant said on the witness stand that any program he could find and remove from a commercially available time-sharing computer system is automatically in the public domain unless some combination of sufficiently protective measures have been taken. The judge in that criminal case concluded that under the facts before the court, adequate protection to meet the secrecy requirement necessary to define the program as a trade secret was given by using an unlisted telephone number, a confidentially assigned user account number, and an unpublicized program file name.

A programmer working for a time-sharing service admitted to legitimately buying time from competitors and then attempting to take copies of programs, customer list files, and other users' files, and

to penetrate the protected operating system, and finally to cause a disruption or breakdown of the system. He believed this was not unethical or illegal because he was not constrained in any way by contract, user documentation, proprietary rights statements or the equivalent of "No trespassing" or "Do not enter" signs within the system. Further investigation indicates that this practice is common among commercial time-sharing companies' employees.

There appears to be a growing feeling among certain computer professionals that such activity is a form of reverse engineering—a legitimate business technique in which the product of a secret process is analyzed by persons who have not appropriated the secret improperly, nor are in a confidential relationship with the holder of the secret process. Others would list the same activity as industrial espionage and sabotage, a form of unfair competition, or theft and malicious mischief.

The current low level of agreement among computer professionals as to what constitutes fair practice is disquieting to those seeking standards to follow.

Similarly, and no less confusing to the industry, is the current status of the law of patent, copyright, trademark, and trade secrets as applied to software protection. Most experts agree that the present laws are unsatisfactory. Less concurrence, however, exists as to the right solution to provide some protection to the developer while not impeding necessary progress in this rapidly growing and changing technology.

We can't hope to control and prevent computer related crime until a tradition of ethical standards is established in the edp occupations, along with laws applicable to acts and assets associated with EDP, and regulation through forms of initial protection and licensing. Technological solutions are necessary, but not sufficient.

DATA PROCESSING PERSONNEL MOVE ONTO THE "WANTED" LISTS

According to the Treasury Department, occupations of the principal perpetrators of reported bank embezzlements of all types in 1971 were:

Position

Operations vice president, manager, clerk-----	32
Loan officer, manager-----	29
Teller-----	22
President-----	14
Cashier-----	8
Director, stockholder, officer-----	5
Bookkeeper-----	3
Trust officer-----	3
Auditor-----	1
Computer operator-----	1
Proof department-----	1
Systems analyst-----	1

The principal perpetrators of all reported computer-related bank embezzlements from 1966 to the present were:

Position

Vice president, EDP-----	4
Edp clerk-----	3
Programmer-----	3
Computer operator-----	2
Chief teller-----	1
Systems analyst-----	1
Vice president-----	1

In several of these cases additional perpetrators were in other occupations, but they were in collusion with these edp people who have the skills and access to do the dirty work.

Mr. Parker is a senior information processing specialist at Stanford Research Institute. He has been in the computer field for 23 years in programming, management and research. He has spent the past two years researching computer abuse under a National Science Foundation grant. This article is based on the final report for that research, titled Computer Abuse, which was published in Nov. 1973.

Ms. Nycum is a research associate on leave from Stanford University Law School. A practicing attorney, she is a member of the Pennsylvania Bar and the U.S. Supreme Court Bar. A past director of the Stanford University Campus Computation Center, she has acted as a consultant on the NSF computer abuse study.

[From New Scientist, Aug. 22, 1974]

COMPUTERS NEED PROTECTION AGAINST PROGRAMMERS

(By Hedley Voysey)

The most experienced computer programmers are the people who must be closely disciplined in the effort to ensure secure computer systems. After all, the violators of programming rules are always the ones who set the rules. This is the conclusion of the much-heralded IBM-funded report on data security. It means that students of computer science in the higher educational establishments of the UK can confidently expect to be among observed workers in the world in the next few years.

Routines written by inexperienced members of the staff caused little trouble, says the report. But the programmers who tinker with the control programs of computers (rather than write applications programs) are not to be allowed to change the systems programming environment without the express approval of an independent group of experts charged with responsibility for data security matters.

The report tries to pacify computer software specialists by emphasizing that this "supervision" is merely to protect them from unwarranted accusations and suspicions of illicit actions. Since it is the unintended results of a control program change that can cause a breach in security, the point is well made. But the hard fact remains that executive awareness of the power of control program changes will throw a cloud over many budding computer specialists.

The 1200 pages of the report, "Data Security and Data Processing", is the result of four study groups working at the behest of IBM. In May 1972 IBM ran its public concern flag up its prominent flagpole with the news that it was to spend some \$40 million over the next four years in tackling the data security problem (New Scientist, vol. 58, p. 812). The currently available report is the result of about 10 per cent of this cash (the rest being swept into the product development plans of IBM). The usefulness of the report is based on the skills of professionals working at Massachusetts Institute of Technology (MIT), TRW Systems Inc., and the Management Information Division of the State of Illinois. Additionally IBM had an internal study centre at its Federal Systems Division.

The formidable report has its effect compounded out of good statistical, managerial, and computer techniques advice liberally mixed with the kind of black humour that is endemic to computer activities.

The need for wider managerial awareness of the vulnerability of computer processes to security threats is illustrated by the remark of a service bureau manager who indicated that some of his customers are sensitive about the security of data and some are not—but he said “all are naive”. The MIT study indicated that those who know most about computers are most concerned to set security weaknesses right. The long association of computers with the financial world gave this sector of users the highest appreciation of the risks of computer vulnerability.

Arnold Lieberman of MIT contributes a practical guide to data access control through defining ownership of data. His system went into action at MIT on 25 February, 1974. He concludes laconically that if anything can be learned from the MIT experience; “It is that the sudden and abrupt transition from no security to full security is not only possible, it is not even particularly difficult.” The same author, however, notes five pages earlier that the first attempt to introduce monitoring caused the daily accounting run to fail for lack of space in its intermediate work. He says “The sensitivity of the accounting function is so great that this fiasco resulted in many weeks of delay before monitoring could be run full time.”

Computer researchers can take comfort from the general conclusion of the study that operating systems must be written in a less opaque form in the future and from the contention embodied in the report that abstract machines are inherently more secure than real machines. Since the design of abstract computers (or virtual machines) which can be realised on actual physical hardware is a major research topic, it seems that the (potential) computer burglars in more academic environments are still the main hope of the potential buyers of safely locked-up data processing systems.

[From *Dimensions/National Bureau of Standards*, July 1974]

PRIVACY AND SECURITY: TWIN CHALLENGES TO COMPUTER TECHNOLOGY

Mention the sophistication of computers and computer systems and their vast use these days and you're likely to open a Pandora's box. Out flies technology as a blessing—and a curse. Easily accessible information can facilitate business transactions and assist communications. It can serve a critical need by rapidly providing medical data. But on the negative side, the deep-rooted and irrational dread of mechanical “brain power” fuses with the real threat of unrestrained information gathering and dissemination.

Dr. Ruth Davis, head of the National Bureau of Standard's Institute for Computer Sciences and Technology (ICST), states the situation like this: “There is a societal problem today that signals a major confrontation between the individual in modern society and modern technology. It is the problem variously referred to as that of ‘Invasion of Individual Privacy,’ ‘Data Security,’ or ‘Computer Crime.’”

She sees several possible results from the impending conflict: It could “. . . trigger off negative chain reactions as well as possibly

damaging restrictive controls on many applications of technology." Or, if the various branches of Government and industry treat the problem lightly, ". . . then computer and communications technology could indeed victimize individuals and intrude upon their rights as citizens and consumers."

INSTANT INFO

The hum and stutter of nearly 144,000 computers in the United States alone signal isolated pockets of data or whole networks of information systems capable of instantly relaying data coast to coast. Who controls the data gathering, who decides it's valid, who has access to it, how do we know it can't be tampered with?

The right of privacy is a legal matter. That right is not spelled out in the Constitution, although privacy cases have been prosecuted under other rights. But states like California have already begun to act in favor of the individual by passing laws on privacy.

On a national level, the President's Committee on the Right of Privacy, chaired by Vice President Gerald Ford, is surveying the situation and will come up with recommendations.

Davis heads one of the Committee's 10 task forces; Robert Blanc, an ICST computer specialist, serves on another.

In addition, NBS has sponsored two conferences on privacy and computer security—one in November, 1973, and one in March 1974. These meetings brought together parties involved in the various aspects of the privacy/security question, including the legal and the technological. The purpose was to get an overview of the entire spectrum of activities and to foster coordination at all levels.

Representatives from Government, the computer industries, consumer groups and academia attended and participated. Congressmen Barry Goldwater, Jr., (Calif.) and Edward I. Koch (N.Y.), both sponsoring separate legislation on privacy, presented their views at the March conference. Since that time, they have cosponsored a bill that would define information practices to be followed with respect to personal data files maintained by Federal agencies.

Whether or not the rights are defined and listed, at least one facet of the technological problem must be confronted: computer security. Finding ways of protecting computers from physical damage or manipulation and of protecting data and the access to it require the aid of science and technology.

SECURE ?

At present, how secure are computer systems? Clark Renninger, ICST's staff assistant for computer utilization programs, feels that a poll of experts would probably produce the consensus that, "No system on the market today is a secure system." Why? Because security has never before been a design priority.

That picture will probably be changing soon. One main mission of ICST is to provide automated data processing standards for use by the Federal Government. With its more than 7,000 computers, the U.S. Government is the largest single computer user in the world. With Federal emphasis on privacy and security and with NBS coordinating with industry and consumers in developing secure systems

and security standards, the results of their efforts will extend into both the public and private sectors.

A main drawback to the easy assimilation of security technology is a perennial hang-up—money! It's going to cost plenty. As an example, Davis has used a model of a hypothetical credit reporting agency. This agency, beginning with 1 million records containing 220 characters of data each, would have an average file growth of 10 percent per year—33 million additional characters annually. That's just to meet the requirements of pending security legislation, and it discounts growth of the agency. In 7 years the size of the file would double, software checking procedures would require implementation and processing time for each query would increase. Larger files would also mean more hardware. The cost rise would be significant.

Critics of computer security say that security at a high price is not necessary. They admit that at present the potential for unauthorized persons to gain access to files or to alter data is vast. But they cite statistics like those of a Stanford Research Institute study showing that documented transgressions are few.

On the other hand, computer crime is difficult to discover, and it's more difficult still to find the offender. Davis feels that costs could be spread among supplier industries, service industries, the consumer public and Government, thus easing the burden through sharing.

Davis also states, "Paying for privacy and security is not new to the American public. Some 15 percent of the 100 million telephones in the United States have unlisted phone numbers. The American public is currently paying \$150 million for this right." She cites other examples: security apartments, private physicians, private housing.

FINDING SECURITY

If indeed we want security, we can't come by it simply, regardless of cost. Davis summarizes the problem:

Threats to information systems range over a broad spectrum including events such as: natural catastrophe, sabotage, theft, bugging, accidental disclosure and physical assault. The countermeasure spectrum is just as extensive, for example: physical barriers and guards, passwords and identification badges, data encryption, audit trails, personnel practices, backup copies of data and access control software. Not all threats will exist for each system, and not all countermeasures are appropriate to counter each threat. Each information system must be analyzed to design an adequate security environment.

It is only when armed with these types of data and knowledge that an appropriate approach to the problems of data confidentiality and security can be formulated.

NBS is already taking action to make computer security a reality. By the fall of 1974, ICST intends to provide a set of guidelines for achieving physical security within Federal automated information systems. This should provide safeguards for computer equipment. NBS is also completing an initial survey of Federal practices in providing for computer security which will be published this year.

Safeguarding the system and the information itself is much more difficult. Supporting science and technology is not yet adequately de-

veloped for this purpose. But R&D is in motion both in Government and the private-sector. NBS is attempting to determine whether operating system software can control access to data. Ways of foiling the biggest threat to computer security—human ingenuity—are being examined. Unique identification methods like voiceprints, memory passwords and fingerprints can reduce the number of people who can gain access. And such methods can better pin down the identity of those who have access to computer information so that the computer criminal cannot easily shield himself in anonymity.

Other problems persist. For example, one person may have a right to certain information stored in a computer, but not to all. It is necessary to restrict, as well as to prevent access.

Data encryption can provide a safeguard in cases where unauthorized access does succeed. By translating information into mathematical systems (algorithms), decoding becomes difficult. ICST has wrestled with the challenge of developing these algorithms to the point that they provide a maximum level of security. NBS is in the process of making these simple algorithms generally available. Making the algorithms available, by the way, does not give away a secret. The system can be used to make unique codes.

Even with the efforts underway in Government and industry, Davis sees that, "The privacy problem has already introduced serious stresses between society and technology." She feels that perhaps the only first step in solving the problem lies in the acceptance of responsibility by Government, the service industries and the courts. She says, "That first step is what we are striving for today."

[From American Bar Association Journal, April 1975]

COMPUTER ABUSES RAISE NEW LEGAL PROBLEMS

(By Susan Hubbell Nycum)

Along with its many benefits, the computer has opened a Pandora's box of abuses. Some computer system abuses do not fit easily under traditional legal concepts, and others are almost impossible to detect. The stance the legal profession takes toward computer abuse will be critical to the development of effective deterrents, detection, and sanctions.

The specter of a nationwide computerized data base of personal information has become a disquieting byproduct of our burgeoning computer society. Timely warnings from Arthur R. Miller's *The Assault on Privacy*, Alan F. Westin and Michael A. Baker's *Data Banks in a Free Society*, and the recent report of the Health, Education, and Welfare Secretary's Advisory Committee on Automated Personal Data Systems have alerted decision makers and the public to the dangers to personal privacy from computerized data banks. The resulting concern has led to the passage of P.L. 93-579, the Privacy Act of 1974, and extensive proposed legislation and administrative action that seek to control the collection and dissemination of information on individuals. Yet privacy intrusion is only one of several important types of computer-related, societal abuse.

As a result of a study supported by the National Science Foundation and conducted at the Stanford Research Institute, four other major computer-related abuses have been identified: abusive acts to computer systems themselves; abusive acts to computerized assets, *i.e.*, programs and data; abusive acts in which the computer is used as a symbol, such as in consumer frauds; and abusive acts in which the computer is used as the perpetrating device or instrument.

These abuses have been categorized as a result of examining more than two hundred incidents collected over an eight-year period by the study's principal investigator, Donn B. Parker. Although the number of incidents is small, they should be viewed as the tip of an ever-expanding iceberg. These abuses are such that probably many go completely undetected, and many others are not reported by their victims.

While categorizing the events, the researchers also analyzed them for several additional factors. These included adequacy of technical deterrents and detection mechanisms, social attitudes toward computers, efficacy of existing laws to protect proprietary interests and those of society generally, technical skills necessary for management, law enforcement, auditing, and other personnel involved in the deterrent and detection process, and information required for participants in the legislative and judicial process who are called upon to address the issues of sanction and remedy.

The study showed that crime and civil abuses occur across a wide range of computer activity. Assessment of control efforts emphasized that bare technical restraints will be no more effective here than in the more restricted domain of computer-related privacy intrusion. As in privacy considerations, however, the legal community will be critical contributors to the architecture of effective deterrents, detection, and sanctions to these computer-related, antisocial acts.

STUDY EMPLOYED INTERDISCIPLINARY APPROACH

An interdisciplinary approach was taken in the study. In addition to Mr. Parker, a computer scientist, the primary research team included Stephen Oūra, a sociologist, and me. Initial hypotheses were evaluated by another group of specialists including Donald Cressey, a criminologist; John Kaplan, a professor of criminal law and evidence; Tom Crockett, director of research of the International Association of Chiefs of Police; and Philip Enslow, then of the federal Office of Telecommunications Policy. Thirty invited experts met with the researchers to critique the study. In a day-long session lawyers, computer scientists, bank auditors, and computer security people representing government, computer vendors, companies using computer resources, research organizations, and the press discussed the problem with the researchers.

Study conclusions are that all of the types of abuses identified have an important impact on society. A full treatment of each, however, is impossible in a survey article. For in-depth coverage the reader is referred to the project report, *Computer Abuse*, by Donn B. Parker, Susan H. Nycum, and S. Stephen Oūra, Stanford Research Institute, Menlo Park, California.

Abusive acts to computer systems encompass the most violent of the reported incidents and carry the highest risk of danger of personal injury. Direct physical attacks on computer equipment (hardware) escalated during the time of the Vietnam War. Protesters, seeing the computer as a tool of warmongers or the establishment, sought to destroy it or capture it and hold it for ransom until various demands had been met by the victim institutions. In some cases the computer was attacked after the building or room that it occupied was broken into. Then cables were severed and the computer was bludgeoned, set on fire, or flooded. Fire bombings took place, and at the University of Wisconsin an explosion took the life of a researcher. These and other incidents were readily detected crimes not needing any computer *expertise* to establish their occurrence. They were also readily identifiable as forms of vandalism or malicious mischief, burglary, extortion, or criminal trespass.

Also harmful but less obvious activity left the equipment unscathed but damaged the programs (software) and data stored within a system. Vandals equipped with remote terminals, telephone connections, and computer know-how could erase or alter the key programs that enable the equipment to function from locations miles away from the computer itself.

Analysis of on-line software vandalism has exposed one of the primary difficulties with computer abuse. This relates to the equating or expansion of traditional concepts of property and associated definitions of trespass, such as breaking, entering, asportation, deprivation of use, to the activity resulting from the advances of modern electronics. Perpetrators by remote access, for example, did not enter the machine area physically but "broke into" the computer via on-line terminals that were connected by telephone lines and data communication equipment. Do these acts constitute malicious mischief? Is there a burglary? What violation has occurred through the misuse of telephone services?

The theft or misappropriation of computer components is another type of abuse to computer systems. As computers shrink in size and grow in portability (the popular hand calculator is actually a tiny computer), it becomes easier to steal or misappropriate whole systems. Since these thefts are of tangible property, they do not present unique questions of law.

The wrongful taking of computer time from a system is more difficult to categorize as a traditional theft, yet computer time has great value. Stanford Research Institute sources indicate that all but the smallest businesses use in-house or service bureau computers and that 60 percent of all banks would be under severe constraints in opening for business each morning unless their demand deposit accounts had been done successfully on computers during the previous night. Computer time is expensive and an important resource of these businesses. Client firms with in-house computers should be aware of the possibility of employees' running private service bureaus on the company system or performing programming jobs for outsiders on their overhead usage accounts. Those who buy time from time-sharing networks or service bureaus should know of the technical ease with which an

unauthorized person can gain access to a system through forged user credentials, such as key words or user account numbers, that result in billings to a legitimate customer.

ABUSIVE ACTS TO COMPUTERIZED ASSETS

The second identified area of computer abuse concerns abusive acts to computerized assets, *i.e.*, programs and data. This includes unauthorized use of programs and data and unauthorized alteration thereof. Unauthorized use of computer programs, some worth millions of dollars in development costs, is a major threat to owners of proprietary software.

In *Ward v. Superior Court of the State of California, County of Alameda*, 3 Computer Law Service 206 (1972), the superior court found probable cause that the defendant had stolen, taken, or carried away an article representing a trade secret. The trade secret consisted of a computer program, the tangible article was a copy of the program Ward caused to have printed out by his employer's computer and that he then carried to his office in violation of Section 499c(b)(1) of the California Penal Code. The court further found probable cause in that having unlawfully obtained access to the program, without authority, the defendant made a copy consisting of two print outs of an article that represented the trade secret, in violation of Section 499c(b)(3).

Some interesting questions posed by software misappropriation or theft concern its form. Unlike most other types of property, software can be carried away or converted by copying. Although the owner remains in possession of the program, an unauthorized person can have possession of a duplicate. The concurrent possession dilutes the control over the property and thereby may lower its value.

It is suggested that the emphasis in these cases be on loss of control or breach of a fiduciary relationship rather than on a traditional property concept of denial of use. This approach also avoids the necessity of finding a taking or the making of a copy in tangible form. A program is capable of being sent from computer to computer and being used without ever appearing in hard copy form. In the *Ward* case, however, the court found no violation of Section 499c of the California Penal Code (theft of trade secrets) in the mere transmission of electronic impulses over telephone wires.

THE COMPUTER AS A SYMBOL

Instances in which the computer appears as a symbol are those concerning consumer abuses, such as fraud. The cases in the Stanford Research Institute file involve disputes over computer processing of insurance policies, fraudulent use of mailing lists, unfair billing practices, and dating services and trade schools engaged in false advertising.

THE COMPUTER AS A PERPETRATING DEVICE

While each of these abuses is harmful to society, the highest incidence of loss occurred when the computer was used as the perpetrating device in a criminal activity.

The speed of a computer, its capability of manipulating huge amounts of data, and the differences between the man-machine interaction and the man-paper interaction in recordkeeping have tended to alter the mode of certain business abuses and to provide an attractive environment for the technically skilled, unscrupulous adventurer. Stanford Research Institute sources report that 3 to 7 per cent of the present work force interact directly with computers, while a much larger percentage deals indirectly with them. As a result the possibility for wrongful use is proportionately widespread. While the abuses are traditional, the mode of perpetration is new and can be best understood from an operational viewpoint. In terms of the computer activity these matters can be classified as input, processing, output, and control.

Computer Input

Input refers to data capture, *e.g.*, keypunching, optical character recognition, and the entry of the data into the system in machine-readable form. The possible abuses included in this function are omission of documents, creation of entirely false records, and the altering of amounts, names, and the like, on otherwise authentic documents. The incidents in the project files range from the case of the kindly keypuncher who failed to include her friends' parking tickets when creating the master file of traffic violations for her municipality, to the alleged creation of records representing \$2 billion of nonexistent insurance policies at the Equity Funding Insurance Company in Los Angeles in 1973.

Computer Processing

Processing refers to the manipulation of information within the computer. Abuses include transfers between files, such as bank accounts, and covering up of information contained in files. One of the earliest reported cases, in 1966, involved a programmer who put in a change to the computer system causing it to ignore overdrafts on his account. He was convicted of, and given a suspended sentence for alteration of bank records—the first nonbank employee to be convicted of this crime. He was employed by a programming firm performing the computer services for the bank.

Computer Output

The abuses in the output of computer-generated information, such as print outs and terminal displays, include the employee who hit the repeat button on the printer and caused multiple copies of his legitimately prepared pay check to be printed. He was detected by a bank teller who found his presentation for payment of the multiple copies irregular.

Computer Control

Another form of abuse springs from a control capability over the total system. A number of perpetrators have had to have this type of capability to implement their schemes. Included here are the Union Dime Savings embezzlement of \$1.5 million in 1973 and the alleged massive Equity Funding fraud. When an individual has been able to accomplish his goal unaided by others, it is frequently because of his higher level of supervisory responsibility. One lone perpetrator was

a vice president of his organization before his activities were discovered. Some opportunities for unassisted activity come from lack of separation of functions or lack of controls over access to separated functions. Other acts are possible only through conspiracy. In a New Jersey case bank employees and outsiders worked in concert. The outsiders opened accounts. The insiders transferred funds from little-used accounts to the accomplices' accounts. Then the accomplices simply withdrew from their accounts. The insiders intended to alter the bank records to conceal the transfers, but a fortuitous computer conversion by the bank, which caused a temporary return to manual processing, occurred before this could be accomplished, and the transfers were uncovered.

Control also can be defined as an affirmative activity by management, auditors, and, when applicable, government officials. The computer has made the audit and reporting function both easier and more difficult. One could argue that a different standard of performance in terms of procedures employed to carry out one's responsibility has been thrust on these groups by virtue of the computer. A computer-prepared report may be the best source of information to raise suspicions of untoward acts, yet in numbers of cases these records were not scrutinized by management until after the perpetrator had been exposed for other reasons. At the same time undue reliance on a computer report and failure to examine both the existence and veracity of these data may subject overcredulous persons to liabilities under the securities, banking, insurance, and corporation laws and, increasingly, for common law negligence.

PERPETRATOR PROFILE ALSO SOUGHT

In addition to categorizing the incidents, the researchers were interested in learning more about the individual perpetrators and the present mechanisms for control available to protect potential victims.

The perpetrators were found to have superior intelligence, to be highly motivated in both theoretical design and field applications, and, in general, to be young—eighteen to thirty years old (exceptions were a few of the embezzlers and some of those involved with business fraud who were older). Few women were found among the perpetrators, but when they were, they usually were keypunch operators or clerks. The elements of challenge and game playing seem to be significantly stronger among computer-abuse perpetrators than among other white-collar criminals.

In some cases, claims of victims that their computer systems were safe and could not be penetrated encouraged programers, who look upon their work as an intellectual challenge pitting their minds against the intransigent machine. One perpetrator, who claims to have gained over one million dollars from his deeds, said that aside from making money rapidly his motive was to see how far he could go with his crime before he informed his victim of the acts. He was confident that no evidence of his act could be found even if he revealed how he did it.

The Robin Hood syndrome is common. One interviewed perpetrator indicated that doing harm to people is highly immoral, but since government-regulated industry in general and telephone companies in

particular do great harm to society, harming these organizations is fair. This differentiation between doing harm to people and to organizations has some current popularity. The computer within the organization is an additionally attractive and satisfying target capable of sustaining loss but not possessing emotional reactions that might produce feelings of guilt in the nonprofessional criminal. Perpetrators strongly fear unanticipated detection and exposure, however, for this would cause great embarrassment and loss of prestige among their peers. The study contains no incident of repetition by a perpetrator who had been exposed.

CONTROL MECHANISMS NOW AVAILABLE

At the present time the advantage in escaping detection is clearly with the perpetrator in terms of technical deterrents and about equal with respect to technical detection. Computer security is a young field; concerted efforts have been made only within the last five years, yet computers themselves have been in use for nearly thirty years. There is a body of shared knowledge much older and more widely disseminated in how to understand and use hardware, operating systems, and applications programs than there is in how to anticipate and deter their misuses. Although enormous efforts are being expended now by vendors to secure the operating systems on their computers (I.B.M.'s announced budget is \$40 million over a five-year period), at present these systems are vulnerable to penetration by persons with systems programming skills.

The operating system is the master control program and the executive or supervisor who controls and schedules processes within the machine and to and from its peripherals. The most sophisticated systems are as vulnerable as the simple ones. University installations, which traditionally are the most complex systems, also report a high frequency of system breach. The complexity and cleverness of these intrusions would tend to indicate that a degree in computer science is necessary to compromise a system. Yet the media carry stories of high school students and younger persons who have obtained time on a computer and, through curiosity and perseverance, cracked its internal security, played havoc with its programs and data, and finally caused its operating system to fail.

ABSENCE OF CONSTRAINTS IMPLIES PERMISSION

Until these systems are more secure, no amount of precaution taken with application programs or physical security will be sufficient. Even when the ongoing efforts in system security result in tighter systems, which are predicted for the next two to six years, there still will be a coterie of computer professionals capable of abusive activity. A provocative attitude exists among a number of highly skilled, generally moral programmers; penetrating another's system to see how it works and what its weaknesses are, to the point of crashing the system, is reverse engineering. Their opinion is that in the absence of explicit constraints, such as contract provisions or notice of proprietary rights stated within the system, knowledge is power and no unfair, unethical, or illegal practices are involved.

Detection capabilities are likewise impeded by vulnerable systems. The presence of a critical command sequence secretly lodged within an innocuous program, which will be activated when the innocent program is finally run, may prevent or at best postpone detection by even highly skilled computer people. This technique, appropriately named the Trojan horse, is only one of the obscure ways a system can be contaminated. Auditors are particularly handicapped. This creates a situation all the more unfortunate because these professionals have taken giant strides in upgrading their technical skills to meet the imperatives of automated recordkeeping.

[From the Journal of Accountancy, February 1975]

EDP ACCOUNTING

(By Robert L. Stone)

Robert L. Stone is manager of software applications in the AICPA's computer services division. This article is adapted from a speech he presented at a recent meeting of the IBM Accountants Computer Users Group, ACUTE.

One positive sign of man's existence comes from an unlikely source—his ability to commit criminal acts no matter how difficult the circumstances. The famous escape artist Willie Sutton, who had the ability to free himself from escape proof prisons and the equally famous magician Houdini, who amazed the world with his ability to escape from any confinement, both proved that no technology can thwart the ingenuity of a clever mind.

Another positive sign of man's existence lies in what appears to be a basic rule of life: As soon as a new invention appears, someone, somewhere will try to develop a method of beating it. This rule is particularly true in the computer field. The black box seems to affect many people in the same way a red flag affects a bull. For five years I was associated with a university. One of my students in a basic programming course became so "turned on" by the computer that he spent every available minute at the computer center learning all he could about it. His hobby was trying to break the operating system. He eventually did so despite the efforts of some brilliant computer scientists who were trying to stop him.

The computer has been with us since the early 1950's. There are over 110,000 computers in use today and at least 80 percent of them are being used to keep financial records. During this 20-year period, there have been approximately 225 reported cases of computer abuse. Some security experts say the actual number is twice that, because many companies who are victims of such abuse do not report it.

When a case of computer abuse is uncovered, who is responsible? Who should be held accountable for the assets lost?

Should it be the auditors? Perhaps they did not use the various tools available to them to audit a client who used a computer to record financial transactions.

Should it be the data processing manager? He has certain tools available to aid him in managing his center and, if he did not use

these tools, he may be held responsible for the actions of his subordinates.

Should it be the computer vendors? Perhaps they supplied a computer that had no security controls or had controls that could so easily be bypassed that they were, in effect, meaningless.

No security system is perfect. A recent article reported the destruction of a computer center which was considered to be indestructible. It was built away from a metropolitan area; it had the most up-to-date fire and smoke detecting devices; and employed a sophisticated physical security system. In short, it was a perfect example of a secure data center. One day, the center was completely destroyed. Someone overlooked the potential hazard of locating the building in the flight path of a large airport. A pilot, misjudging the runway, crashed his plane into the center.

The July 1974 issue of *Fortune* contained an article "Waiting for the Great Computer Ripoff" that described how two men broke the security of MULTICS, Honeywells' most sophisticated security system. A few simple instructions by a terminal operator 3,000 miles away completely subverted every one of the system's safeguards, giving the operator complete control of the system.

These are only two examples which prove that no computer center is absolutely safe. The unexpected can and does happen. But how many of the reported cases of computer security break-downs can be attributed to these kinds of destruction or abuse? How many of the more than 148 fraud cases reported by Donn Parker, of the Stanford Research Institute, in his study of computer abuse were caused by the physical destruction of a data center? How many of the more than one million programmers in the United States are as intelligent and as dedicated as the two men who broke the security system of MULTICS? Of those who are as intelligent and as dedicated, how many are willing to put their knowledge to some illegal use? According to one security expert "Almost all computer-assisted fraud is so simple and straightforward that it makes you wonder what the really smart (and as yet undetected) people are doing?" How true is this statement? If you talk to a number of EDP auditing control experts you will find that they think it is very true. The synopsis of the 148 cases reported by Mr. Parker also tends to support the statement. Monday morning quarterbacking always produces better results, however. I firmly believe tools are available that could have been applied by the auditors and data processing managers involved that might have detected most of the fraud cases reported.

The data processing manager does not have professional guidelines like those of the CPA, so he is in a more vulnerable position if he has to defend himself in court when his computer is used illegally. Lawyers point out that corporate officers may legally incur personal liability to the company and its stockholders if, through their neglect or oversight, such a fraud should occur. Should he be held liable if he did not use some of the tools available to him? To illustrate, the Equity Funding indictments involved the data processing manager and several other EDP employees.

Even the computer vendor will not escape the wrath of a dissatisfied public. He has a responsibility for providing a secure computer system. This was recently demonstrated in the Equity Funding case

when a stockholder class action suit was filed against IBM for providing a computer that could be used to help create such a massive fraud. The case was dismissed before the trial began but the next one may not be so easily resolved.

All of this leads to the belief that the next fraud case involving the computer may find all three of the groups as defendants in a court of law. What tools are available and can be used in providing a more secure data center? The following is a partial list of those I have found. As I discuss each item, you might think of an appropriate defense you could make to a jury if you did not use that tool in your data center.

COMPUTER VENDOR

As a supplier of hardware, the computer vendor has a moral and legal obligation to furnish a machine that has built-in security devices that will protect the user from injury or loss. Any manufacturer who supplies unsafe equipment may be liable in the event someone is subsequently injured. A computer vendor may be liable for damages when his computer is used illegally if he did not build in security devices to prevent such usage.

Many vendors have supplied a computer with an operating system that is so full of security leaks that the good security features that are built into the system are rendered useless. Security features like password protection, header and trailer labels, and systems to record operating statistics are excellent features. However, when the vendors provide documentation that shows a good programmer where these features are located, they have given him the ability either to bypass them or remove them from the operating system. It is not enough merely to provide these features, the vendors must implement them in such a way that they cannot be circumvented without great effort.

A leading security expert recently stated that there really would not be a good, secure computer system until the next generation of computers is available. Present-day computers do not have elaborate security features built into them because security was not considered to be a major problem when they were designed. The vast majority of today's computers do not possess the security features that they would need to meet the data confidentiality conditions required by some of the pending data privacy legislation. What about the additional 110,000 computer that some experts say will be installed before the next generation of computers comes into being? It seems likely that they will also lack the necessary security capabilities.

What can you do to help make your computer more secure? Here are a few suggestions:

First, initiate a massive advertising campaign to inform the business and general public that security features are built into your systems. Many people, especially top management, do not know these features exist.

Second, as a part of your customer engineers' job of preventive maintenance, have them check every computer system sold to determine if the security features provided have been bypassed or eliminated from the current operating system. If they have been eliminated, notify top management of the fact they are not using these features.

Third, whenever a new system is installed, insist that the security features be a part of the operating system. If they are removed at system generation time, ask for a letter from the user specifically stating that they do not choose to use the available security provisions.

Finally, when the next generation of systems is released, make the security devices a permanent part of the operating system. Make it impossible to eliminate them or bypass them without spending a great deal of time and money.

These may sound like drastic steps. However, remember the vendor is as responsible as the auditor or data processing manager for providing a secure system. These suggestions are one way the vendor can meet his obligation.

DATA PROCESSING MANAGER

The data processing manager is responsible for the security of the data center. This security can be classified into either physical security, the physical protection of the center, or operating security, what some people refer to as software security. This article will not deal with physical security. A number of excellent books, articles and pamphlets have been written on this subject. If you have not implemented some type of physical security in your data center, you should do so immediately. Two very good treatments on this subject are IBM's *The Considerations of Physical Security in a Computer Environment* and James Martin's book *Security, Accuracy, and Privacy in Computer Systems*.

I would like to discuss operating security because little has been written about it. The recent rash of computer related scandals has made it clear that there is a real threat to the corporation from inside the computer center itself. Systems people have highly specialized skills. These skills, coupled with easy access to operating hardware and programs, can be used to rob or defraud a company in such a way that the crime can go undetected for months, perhaps forever.

Here are some of the tools available to monitor data center activities:

Systems measurement

Your operating system has the capability to detect and report:

- Unscheduled runs.
- Unauthorized access to data files.
- Unauthorized user identification.
- Misuse of the system during testing.

There are various names given to this capability. For purposes of this article I have called it systems measurement. It attempts to answer the following questions:

- Who is doing what?
- For how long?
- How?
- When?

This is by far the most powerful tool available. Every use of the computer system, whether it be to test a program, run a job or copy a file, is recorded by the systems measurement facility. This tool alone would have helped detect over half the reported computer frauds. There are computer programs available that can analyze the mass of

statistics captured by the operating system and prepare meaningful reports for analysis. IBM's SMF system output can be analyzed by using ABACUS from Time Brokers, Inc., or SMS/CAS from Boole & Babbage. I am sure there are other packages as good as these for other vendors' hardware. Every data processing manager should use this tool.

Segregation of duties

More than half the recent computer fraud cases involved collusion. This is a far greater incidence than in manual frauds. This may mean that computer fraud requires more skill, access and knowledge than is possessed by any one person. If this is true, then the need for separation of duties within a data center, takes on greater meaning. Have you properly segregated the operating and development activities in your data center? Do you require your key personnel to take two consecutive weeks vacation? If separation of duties is impractical, do you provide dual control over sensitive functions? Segregation of duties was an important control in manual systems. In EDP systems it is vital.

C Program verification—Several recent computer frauds occurred because a programmer changed a production program. Do you ever compare a production program with the original one that you approved? Just the idea that you periodically make such a verification would, in a lot of cases, keep your programmers honest.

D Psychological tools—There are other tools inexpensive to initiate. I would like to categorize them as psychological security tools. They do not add to the security of your data center, but they do promote an atmosphere of security. Martin's book lists the following:

1 Information and training—Make security responsibilities clear to your people. The object of security education must be to obtain security by consent. It should never be imposed without reason.

2 Ensure that security is taken seriously—Employees should be immediately apprehended for any breaches in security. If an employee knows he will be in trouble when caught, he will be less likely to make a game of trying to break the security system. Above all, you must be a model in taking security seriously. If you let classified reports lie around, do not lock your desk drawer and do not bother showing your ID card to the guard because he knows you, do not expect your employees to follow the rules.

3 Monitoring the observance of security rules—Security, being negative by nature, involves a natural inertia. Left alone it will be forgotten. You should walk around your data center after hours to see if drawers are locked, classified documents are put away, tapes and disk files are properly stored in the library, etc. Your employees must know that management is serious about and alert to security breaches.

4 Morale—When morale is low, risk to security becomes high. Get to know your employees. Be sure your employees are kept well informed of company policy. Include your key employees in decisions that may affect their jobs. Set up a suggestion box and respond to the suggestions.

5 Be careful when firing employees—We have all heard the "war" stories of EDP employees venting their wrath on their

employers when told they were fired. It is brutal, but the only safe thing to do is ask them to leave the premises immediately. You might ease the situation by giving them a month's pay to tide them over until they get a job.

Donn Parker offers these inexpensive tools:

Posters

Place large posters in your computer facility informing employees that they are working with confidential information and that it is a criminal offense to remove anything from the computer room. These are inexpensive to set up and are a constant reminder that security is important. Other posters should inform your people what to do in an emergency; provide the telephone number of the police and fire departments and set forth an outline of your disaster plan. Posters provide good psychological security; you should make use of them.

Program ownership

Your source programs should contain a statement indicating the ownership and usage restrictions of the program. A statement to the effect that it is a criminal offense to remove the program from the data center places the user on guard that the program is the sole property of the company.

These are just a few of the tools available to you. Most of them are inexpensive and you should be using them.

AUDITOR

Nineteen seventy-four might be called the year of the auditor. The historical position of the auditor, which seems to be that fraud is not what the CPA is responsible for finding, has to be reconsidered. We have seen too many cases of management fraud where management has obscured the reality of the corporate activity from the auditor. These comments were made by Sandy Burton, Chief Accountant of the SEC, before the Dean's Forum in Los Angeles. If he is right it means that you must use the tools available to you as auditors to aid you in your work. If you do not use them, you will be hard pressed to defend yourself in the event one of your clients falls victim to a fraud.

Here are a few tools that are available to you:

Computer audit software

There are about 50 software packages on the market that can be used for audit purposes. They can be used to help you determine the accuracy of the data files used to create the financial statements being audited. This is the most important tool available to you. It is difficult to understand why any CPA firm that has clients with computers does not use some form of audit software. The typical package will foot, crossfoot and perform all mathematical functions. It will take a sample, print confirmations and prepare almost any type of analytical report desired. All of this can be accomplished by an auditor who does not have to be a programmer or systems analyst. Some packages rent for as low as \$80 a month, on a month-to-month basis, so they are within reach of almost everyone.

Internal control guidelines

Internal control guides, questionnaires and checklists have been used for many years by auditors in determining the reliability of the internal controls within manual systems. The same principles apply to a computerized system. Guidelines are available to help you ask the right questions in a data processing environment. An excellent checklist for auditors can be found in table D.29 of Martin's book.

Other tools

There are a number of tools available to the auditor who has some experience in data processing. Some require more computer knowledge than others but they all should be considered.

Flowcharting

There are a number of automatic flowcharting programs available that will flowchart source programs. The charts will help you analyze the logic of a source program.

Mapping

Mapping is a technique that helps to identify redundant code, and code that is used infrequently in a source program. This is a relatively new tool but it has been used successfully by the Department of Finance, State of California, in Sacramento. They used it primarily to find areas of high use and, by restructuring their source programs, were able to save as much as 75 percent on the processing time of some programs. Auditors might well be interested in instructions that are infrequently executed. They might be the ones that add \$200 per week to the programmer's paycheck.

Test data generators

Several test data generator packages are available that can create files for use in testing a program. This is a relatively new tool, but it is said to be extremely useful.

Tracing and tagging

Through special programming, a transaction can be tagged and traced throughout the computer system. You can trace the logical path of a transaction by using a printed audit trail of the tagged items.

ITF (integrated test facility)

Also called the mini-company concept, this technique enables you to run dummy transactions through the entire system. It can be used to check the operating system, application programs, outputs, data entry procedures and manual processing. For example, did the bill go out? Were the proper items shipped? etc. The nice thing about this tool is that it requires no special setup, no special computer expertise and no special processing run.

These are just a few of the available tools. They may not all be relevant to your needs, but some of them are and you should be using them.

CONCLUSION

At the beginning of this article, I asked you to think of a possible defense you might make for not using the tools I would describe. I

hope you never have to defend yourself, but as auditors or data processing managers involved with computers that do not have adequate security devices, you are in a vulnerable position if you do not use the tools available to you.

The security problem is complex. It will take inputs from people in many disciplines and it requires huge human and financial resources to develop a solution. For the past 15 years the auditor, the data processing community and the vendors have been trying to solve this and other computer related problems. To be truthful, we have done a rather poor job in many respects. Computer systems have been built that contain inadequate security controls, computer programs have been written that are unauditible and audits have been performed using outdated, inadequate tools.

I recently spent a week listening to James Martin lecture about the teleprocessing and data base systems of the future. One only has to listen to him for a few minutes to understand what is in store for us. Huge data bases containing billions of characters will be stored on-line in multiple locations. Distributed intelligence will completely change our present methods of processing data. The more extended use of satellites in data communication will, within the next decade, enable an operator in New York to access a data bank in Australia, South Africa or Greece at about what it now costs to call Philadelphia. We have to start working together if we are to have any hope of controlling these future systems.

A lot of work must be done. The whole area of auditability needs to be researched. What do we mean by the phrase, auditible system? I am sure the computer vendors and data processing community would appreciate a concrete definition of this phrase.

Many of the tools that I have discussed need further research. The flowcharting tool is a classic example. Designed by data processing professionals to be used by data processing professionals, it needs to be modified for use by the average auditor. Tools like tagging, mapping and ITF need further research to determine their true value to the auditor and data processing community. The whole area of segregation of duties in a data processing center needs to be reviewed. Most such controls are applicable only to the largest data centers. What can the small center do? I mentioned dual control over sensitive areas, what areas need dual controls, what jobs can be combined that will give the least exposure to fraud? These are the kinds of problems that need research.

We must all join together to solve these security problems. Some day a clever person will put together a group of professional programmers, systems engineers, accountants, wiretappers and psychologists to pull off the greatest computer fraud in the world. It will not be hard to do and, given today's technology, there is a better than even chance that the fraud will go undetected for a long period of time.

Finally, I would like to quote from a letter I received from a time-sharing company that has a very good security system:

"If you could test a trial password every second, it would take 500 hours to try all the possibilities for a single password. This comes to a

total of 250 working days and about \$80,000! To test all the possibilities for our scramble code would take 150 billion years at one per second. Assuming we don't change our rates, that will cost fifty-two quadrillion dollars."

Is your data center this safe?

MEMORANDUM

JUNE 18, 1976.

To: Senator Ribicoff.
From: Fred Asselin, Investigator.

In addition to the articles selected by the Science Policy Research Division of the Congressional Research Service of the Library of Congress, we have selected a number of other articles which demonstrate further problems associated with computer technology. These additional articles follow:

[From the New York Times, Dec. 8, 1974]

FRAUD BY COMPUTER IS AVERTED ON COAST

(By Robert A. Wright)

LOS ANGELES, Dec. 7—An alleged scheme to embezzle \$2.5-million from the Los Angeles City Treasury was broken up in two arrests here early today.

Agents of the Senate Permanent Subcommittee on Investigations, who uncovered the scheme, said the case might have been the prototype of a plan by organized crime to tap municipal treasuries throughout the country through the manipulation of city computers.

Investigators said that they had not yet determined the full details of how the scheme worked but that it apparently involved the juggling of accounts in the Los Angeles City Administrative Office and the payment of checks by the city's computer to bogus corporations. They said it was logical to assume that someone in the municipal government was involved.

They said that the checks had been routed through accounts in banks in the United States, held in the names of the bogus corporations thence to European banks, which wired authorizations to other American banks for payment.

Arrested were Bernie Howard of New York City, an accountant, and Morton B. Freeman, a Los Angeles area businessman. Mr. Howard has been linked in Senate hearings with Carmine Lombardozi, an associate of Carlo Gambino, reputed New York Mafia boss.

Working on information developed by the Senate subcommittee, headed by Senator Henry M. Jackson, Democrat of Washington, 12 agents of Los Angeles County District Attorney's office made the arrests.

Details of the arrests say only that the two men were arrested at 12:30 A.M. as they left a Beverly Hills hotel carrying briefcases containing what the suspects thought was \$1.2 million, their share of the loot.

Four teams of arresting officers were coordinated by Clayton Anderson, chief of the District Attorney's Intelligence Division, and Stephen

Trodd, chief prosecutor of the District Attorney's Organized Crime Division.

Other arrests are expected, investigators said.

Senator Jackson, who was attending the Democratic party conference in Kansas City, said in a statement issued by his Washington office that his investigators would continue to work with Los Angeles officials on the case.

"I want to know just how deeply elements of organized crime have penetrated local governments' computer systems that are, in effect, the vaults for the money collected from taxpayers," the Jackson statement said.

Senate investigators will "begin to determine whether other cities or governmental entities have been swindled out of millions of dollars," it added.

THREE CHECKS INVOLVED

The office of Mayor Tom Bradley of Los Angeles, who is also attending the Kansas City meeting, confirmed that three checks had been written to the allegedly phony corporations identified by Senate investigators.

The checks, each dated Nov. 18, 1974, were made out to Mercantile Trading Corporation, 30 North LaSalle Street, Chicago, for \$856,729.42; National Equipment Group, 200 Park Avenue, New York City, for \$880,195.12, and to Schaffer Supply Corporation, 1 World Trade Center Building, New York City, for \$826,987.53.

Mr. Howard and Mr. Freeman were questioned throughout the night and booked at 5 A.M. on charges of conspiring to commit grand theft, conspiracy to commit forgery and attempted grand theft. Both men are being held in the Los Angeles County Jail in lieu of \$15,000 bail. Arraignment is scheduled for Monday.

George Stoner, chief of the District Attorney's Division of Investigation, said further arrests depended "on a lot of work to do," but that his office knew the names of the others believed involved in the scheme.

Philip R. Manuel, who heads the subcommittee continuing investigation of organized and white collar crime, said that although details of the computer manipulation had not been established, the chances were "very great" that the scheme would not have been detected without information supplied by a subcommittee source.

Mr. Manuel said it was "a logical assumption" that the scheme involved an operative within the city government.

He declined to provide the names of the banks involved in the transfer of funds.

Mr. Manuel said the subcommittee had information indicating that similar schemes in other cities involved some of the same people suspected of the Los Angeles manipulation. But he said that information had not yet been developed to the point that it had been in Los Angeles.

[From the New York Times, Dec. 10, 1974]

CHECK FOR \$902,000 IN LOS ANGELES SWINDLE PLAN IS CASHED HERE

(By Robert A. Wright)

LOS ANGELES, Dec. 9—At least one of 18 bogus checks involved in an alleged scheme to defraud the city of Los Angeles of several million dollars through computer manipulation was cashed in New York, city officials said here today.

A spokesman for the Crocker Bank confirmed that a check drawn on the Los Angeles city treasurer for \$902,000 was negotiated by the bank's Crocker international office in New York. But it remained unclear to whom it was payable and who has the money.

Investigators said the alleged scheme involved the rigging of the city check-printing computer to cause the issuance of checks to phony corporations—the laundering of funds by transfer through domestic banks and their European branches.

Under the master control of a bank in the Bahamas, a wire authorization would then be transmitted to a United States bank to approve payment. Investigators said the plan may have been the forerunner of an operation by organized crime to defraud municipalities throughout the United States.

TWO WERE ARRESTED

The alleged swindle was thwarted early Saturday with the arrest of two men by agents of the organized crime unit of the Los Angeles County district attorney's office.

Acting on information as supplied by investigators for the Senate Permanent Subcommittee on Investigations, the agents arrested the two as they left a Beverly Hills hotel with satchels that the apprehended men reportedly believed contained their share of the loot from three bogus checks drawn on the city treasurer totaling \$2.5 million.

Investigators for District Attorney Joseph Bush, who are known to be seeking three more suspects, went to the treasurer's office today in an attempt to determine details of the alleged computer rigging.

Charles Navarro, city controller, said that he believed the "massive plots" would have had to involve "someone inside" the city government. The district attorney's office would not comment on its investigation.

NO CITY LIABILITY

C. P. Erwin Piper, chief administrative officer of Los Angeles, said the city had no liability for the negotiated check for \$902,000. He said the city's computer verification system "kicked out" the bogus check last Tuesday and that the city notified the Los Angeles Bank Clearing Association that it would not honor it.

Mr. Piper said the city had five days, under law, to stop payment on any check it issued.

"If anybody made any payment on [a check that had not been cleared] they've got to be out of their minds," he said.

Mr. Piper acknowledged that the alleged scheme appeared to have depended on the cashing of the check within five days of their issuance.

The three checks involved in Saturday's arrests had never entered the banking system, but the two men arrested were reported to have been under the impression that they were picking up \$1.2-million in proceeds from the checks.

Arrested were Bernard Howard, a 47-year-old Yonkers accountant, and Morton B. Freeman, 52, a Los Angeles area businessman. Mr. Howard has been linked in Senate hearings with New York City organized crime leaders.

District Attorney Busch displayed for reporters the three unnegotiated checks following Saturday's arrests. Because the checks lacked endorsements, it appeared that banks had cooperated with the district attorney in setting the trap for the two men.

A spokesman for the Crocker Bank, with headquarters in San Francisco, said that the \$902,000 check was deposited routinely in its New York office on Nov. 21. He said Crocker International acted as collector for the Banque de Paris of France.

Mr. Piper said the \$902,000 check that the city computer detected as bogus bore an endorsement indicating that it was first deposited with the Marine Midland Bank of New York.

CLEARING NOT VERIFIED

An official of Marine Midland said that he had not been able to verify if his bank cleared the check. A spokesman for Crocker said it had no details on the name of the payee or the current whereabouts of the funds involved. But he said Crocker International had telegraphed receipt of the deposit to the Bank of America in Los Angeles on the day it was received. A spokesman for the Bank of America said it was attempting to verify that. The Banque de Paris could not be reached for comment.

The three checks involved in Saturday's arrests had been made out to three corporations that had no legitimate business with the city, Mr. Busch said. The checks, each dated Nov. 18, were made out to Mercantile Trading Corporation, Chicago, for \$856,729; to National Equipment Group, 200 Park Avenue, New York, for \$880,195, and to Schaffer Supply Corporation, 1 World Trade Center Building, New York, for \$826,987.

The arrested men will be arraigned tomorrow on charges of conspiracy to commit grand theft, conspiracy to commit forgery and attempted grand theft. Mr. Busch said he would seek bail of \$100,000.



11/55

TREASURER OF THE CITY OF LOS ANGELES

FUND 7 302 GENERAL DEMAND

16-358 1220

PAY TO THE ORDER OF

MO DAY YR DEMAND CHECK NO

DOLLARS CENTS

CROCKER INTL. BANK OF NEW YORK
72 WALL STREET
NEW YORK CITY, N. Y. 10005
FOR CREDIT ACCT:
BANQUE DE PARIS
(GEN. ACCT. COGESA)

11 18 74 046187 \$ 902,125 13

APPROVED:

CONTROLLER

Charles [Signature]

H 801 990

II

⑆ 220-0358⑆

J-C. CORNAZ

Forster

*Compagnie de Gestion et de Services
Cogesa*

TÉL 80221 32 78 40
TELEX 23059
CABLE COGESA GENEVE

37 RUE DE LAUSANNE
GENEVE I SUISSE

[From the Los Angeles Times, Dec. 10, 1974]

L.A. CHECK SECURITY: WHERE DID THIEF HIT?

LOSS AT HEAVILY GUARDED DATA BUREAU CALLED UNLIKELY; THREE OTHER POSSIBLE LOCATIONS LISTED

(By Erwin Baker)

Could the 18 bogus checks involved in the attempt to defraud the city of Los Angeles of at least \$3.8 million have been stolen from the super security-conscious Data Service Bureau in City Hall?

Tug Tamaru, general manager of the vast computer complex, thinks not.

However, he concedes it is one of the four places where the theft could have taken place.

The unsigned IBM-manufactured checks on which City Controller Charles Navarro's name apparently was forged are kept in a wire cage in the rear of the DSB's 30,000-square-foot Emergency Operations Center in the fourth sub-level floor of City Hall East.

To gain entrance to the EOC—which contains banks of IBM computers for general purposes such as payrolls, police and fire control and car-pool operations—employees and visitors must pass through manually, and electronically operated doors.

As additional security precautions, employees must wear badges with photographs and physical descriptions. Visitors must display temporary entrance badges after being cleared by a security guard in a command post or mantrap just inside the center.

When the boxes containing 3,000 unsigned checks each arrive from the manufacturing site at Campbell, Calif., they go to the city controller's office.

Each box—12 inches deep, 12 inches long and eight inches wide—is sealed with strips of masking tape.

At Navarro's office, the boxes are picked up by DSB personnel. At the EOC, as at the controller's office, they are signed for and logged in.

One box is processed in a 10-day period—about 300 checks at a time.

The boxes are opened and resealed about 10 times—one for each process.

On each occasion, the opening is by computer operators under the supervision of their shift supervisors.

Tamaru said about 20 employees, all with police background clearances, are permitted to open and reseal the boxes.

He emphasized they are all senior computer operators or management personnel and all are "trusted employees."

In order to gain entrance to the cage, the employees must insert magnetically-coated badges into a "badge reader" hooked to a special computer for building security,

The computer verifies the employee's right to enter the cage.

After the computer has given the clearance, the employees gain actual entrance with a special key on a blue plastic ring.

"As far as we know," Tamaru said, "the box from which the 18 checks were stolen was sealed."

"We have never had a report of a box being tampered with," he said.

Tamaru agreed with the observation of a top-ranking assistant, however, that a "good crook would make sure it was sealed."

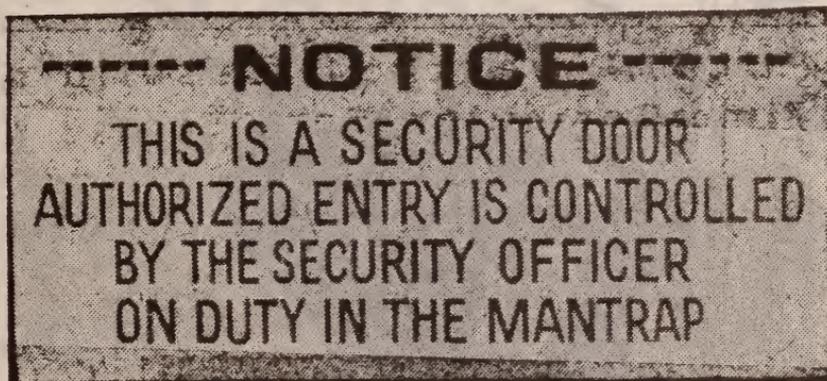
Actually, Tamaru said, while the theft of the checks from the caged area was unlikely, it was one of four possible locations where the theft could have occurred.

The other three, he suggested, were:

—The manufacturer's site at Campbell.

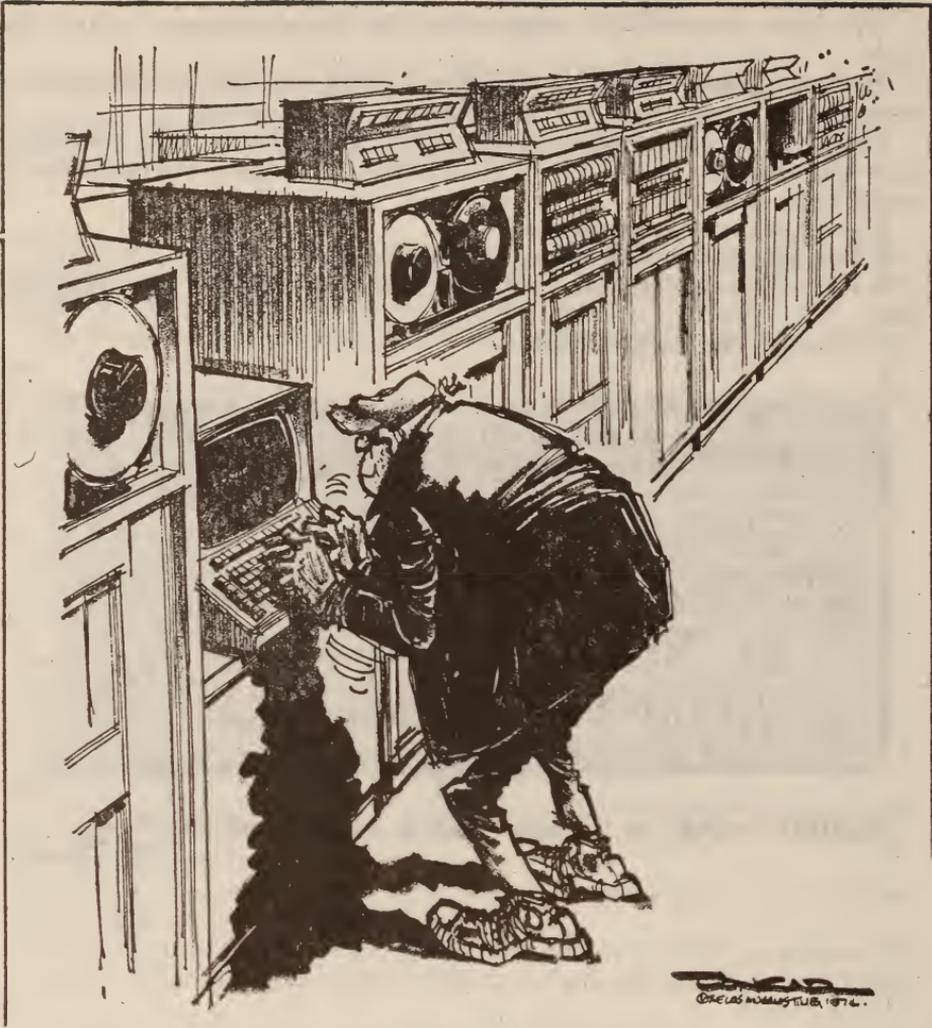
—While the checks were in transit from Campbell to Los Angeles; and

—The city controller's office.



SECURITY—Sign on the door leading to Data Service Bureau.

Times photo



'This is a stickup ...'

[From the Los Angeles Times, Dec. 10, 1974]

[From the Los Angeles Times, Dec. 20, 1974]

CHECKS AND BALANCES—NO PLAN IS FAIL-SAFE

(By John Getze)

What happened to the city of Los Angeles and that bogus \$902,000 check could easily happen again.

And again and again.

Bankers all over the country are now alerted to what happened here—how a person or persons stole blank city checks and passed at least one through the banking system for cash. It therefore seems doubtful that Los Angeles could be "hit" again in the immediate future.

But Los Angeles is not the only city in America, and cities are not the only ones to routinely issue huge checks. Corporations, states and even the Federal Government write thousands of six-figure checks every year, and thus are prime targets for knowledgeable crooks.

Moreover, bankers and corporate treasurers admit they are vulnerable.

"No system is foolproof," a senior Los Angeles bank official said. "No bank or corporation can afford the cost of 100% protection."

The \$902,125 Los Angeles transaction is complicated by the fact that the check was not really a check, it was a warrant. There is a significant legal difference which could be important if the case goes to court as many expect.

Currently, no one is willing to accept the responsibility—or the loss. In fact, the movements of the city's warrant are still being traced.

A major problem in controlling the complex flow of checks and warrants is the growing use of computers and "electronic money"—the transfer of funds by wire or even by telephone.

"Each new piece of technology brings new opportunities for the thief," said the manager of a large Los Angeles company's auditing department. "There are computer crimes that haven't even been thought of yet."

The so-called human factor also is a problem, however.

"Getting auditors or bank tellers to examine the date, amount and signature on each and every check is virtually impossible," said Dan McCarthy, head of Atlantic Richfield's internal auditing department here in Los Angeles.

"It is a very monotonous, tiresome procedure," he added. "And remember, you're talking about one heck of a lot of checks."

According to the American Bankers Assn., approximately 23 billion checks are written every year in the United States.

At Bank of America's processing center here, vice president Larry Cromwell said 4.5 million items are handled every night.

Because of the sheer volume—and the often complicated system by which some checks are processed—forged and even counterfeit checks regularly go unnoticed until the thief has disappeared.

How are big checks normally processed?

"Just like the little ones," Cromwell said.

Suppose you mail a check, written against your account at Bank of America, to the gas company to pay your utility bill. The gas company takes your check and, along with hundreds of others, deposits it in the company's account at, let's say, Union Bank.

Union Bank credits the gas company for the amount of your check, then takes the check to the local clearinghouse association—a place where bankers meet every day.

At the clearinghouse, Union Bank would present the check to Bank of America and, in effect, is reimbursed.

This is a simplification, obviously. There are so many checks, none is handled individually. Bank-to-bank totals are compiled and then the difference is added or subtracted from each bank's separate clearinghouse account.

This is the typical procedure for \$1 million checks as well as \$5 ones, and it is little protection against a good forger.

That is because, barring a highly alert bank clerk, a good forgery would not be noticed until you received the bogus paper in your monthly statement. Incidentally, the bank, not you, would be liable, bankers say.

With large corporations and municipalities, the problem is compounded by the large number of checks written (hundreds or even thousands per day) and the use of sophisticated computer systems.

At one Los Angeles based corporation, two low-level employees recently stole half a dozen blank computerized checks and successfully passed them through the banking system, even though the machine-printed signature was "crudely forged," according to the firm's auditor.

The loss was not great, and the employees were eventually caught—but not until the corporation "reconciled," or balanced, its checking account at the end of the month.

Some corporations are more careful than others.

At one California company, for instance, stolen blank computer checks might not be recognized as missing for up to two weeks. At another Los Angeles company, however, an assistant treasurer said stolen blank checks would be caught in less than 24 hours.

At that second firm, blank computer checks are counted every day.

Both firms added that as soon as a check is discovered to be missing, the appropriate bank or banks would be notified immediately so that "stop-payment orders" could be issued.

Under no circumstances, they said, would bank notification be delayed even for a day, let alone the eight months it took the city of Los Angeles to reveal it was missing 18 such blank checks.

Bankers confirm that immediate notification is standard practice at most major corporations.

Disregarding the delay in reporting lost checks, the case of the bogus \$902,125 city check is unusual for several reasons.

First of all, the \$902,125 city check was not really a check. It was a warrant. And while the two pieces of paper are handled almost exactly the same by the banking system, there is a significant legal difference.

If someone writes you a check for \$100, you can immediately go to his bank and demand payment. That is why, in banking parlance, a checking account is called a demand account.

This is not true with a warrant, however. According to Robert Odell, Los Angeles city treasurer, a warrant is payable only by the city. A bank may advance you the money if it wants to take the risk, but then the bank will have to collect directly from the city.

The city uses warrants to save money. If it were to write a check for \$1 million, it would have to have \$1 million in its bank account—earning no interest. With a warrant, the city can keep the money longer in interest-bearing investments.

“On any one day, we might have \$45 million issued in warrants,” Odell said. “That earns us a lot of interest (up to \$10,000 a day at current investment rates). If we had to have that money in our checking account, we wouldn’t earn anything.”

The case of the bogus Los Angeles check, or warrant, was unusual for another reason, however. Unlike most, the transaction involved as many as half a dozen banks both here and abroad.

Apparently at the center of the complicated transaction was Crocker International Bank, a New York-based subsidiary of Crocker National Bank in San Francisco. Because of legal limitations, Crocker International cannot accept deposits—it can only set up international or nationwide loans or act as a correspondent for other banks. And that is exactly what it was doing in this case.

Ward Stevenson, a Crocker National spokesman in San Francisco, said this is the way it happened:

“Either by mail or messenger, we don’t know which, Crocker International received in New York a Los Angeles city check (actually, of course, a warrant) for \$902,125. The check was made out payable to Crocker International, so it required no endorsement.”

“To the check was attached a piece of paper instructing Crocker International to transfer the funds to an account (Cogesa Co.) at the Banque de Paris in Geneva, a correspondent of Crocker’s with which we do a lot of business.”

Most large banks regularly maintain accounts at other banks throughout the world. So all Crocker had to do was send a wire to Geneva, telling the Banque de Paris to take \$902,125 out of Crocker’s account there and put the money into the Cogesa’s.

Crocker assumed it would collect the \$902,125 from the city of Los Angeles in the near future.

For some reason, however, it took that Los Angeles city warrant 15 days to find its way back to the city where, according to local officials, it was “kicked out” by the computer as being unauthorized.

Four bankers said they could not understand what took so long. The city has offered no explanation either.

But it points out, rather dramatically, that the checking system has substantial loopholes.

“It was a routine transaction,” said Crocker’s Stevenson. “We are a regular correspondent of Banque de Paris and we process numerous transactions for them. We just complied with the instructions.”

What is more, Stevenson said the signature on the \$902,125 city warrant was “perfectly legitimate. In our opinion, it was not a forgery.”

Said another West Coast bank official: “Stealing money by mail is a great way to do it. Nobody can catch you because you aren’t even there.”

[From the New York Times, Dec. 29, 1975]

WOMAN IS GIVEN 94 YEARS IN PLOT TO BILK LOS ANGELES

LOS ANGELES, Dec. 27 (AP)—A motel operator was sentenced to a maximum of 94 years in prison yesterday for her role in a plot to bilk the city of Los Angeles of more than \$3.5 million.

In sentencing Joyce R. Lewis, Judge E. Talbot Callister of Superior Court told her he believed that she could lead the authorities to persons inside city government who participated in the scheme.

Mrs. Lewis, 44 years old, was convicted Dec. 4 on 12 felony counts in connection with the case, which involved cashing stolen city checks made out to fictitious persons.

Two men have also been convicted for their part in the plot—Morton Freeman, 47, formerly a Palos Verdes businessman, and Bernard Howard, a 52-year-old accountant from Yonkers.

A third man, Richard Keats, 39 of Fort Lee, N.J., is being held on \$1 million bond pending trial.

[From the Wall Street Journal, Mar. 12, 1976]

LARGE LOAN SWINDLES SPREAD WITH RELIANCE ON CENTRAL DATA BANKS

(By G. Christian Hill)

ANAHEIM, Calif.—In a squat concrete building on the outskirts of town, a bank of IBM 370 computers receives, stores, updates and distributes credit information on about 50 million Americans.

If the past is any guide, those 50 million Americans include at least a few phantoms, undetected by the computers. Despite tight security measures, con men and fraud rings have devised schemes to feed phony credit histories and identities into the computer files. And they have been able to doctor credit references of actual people to turn poor loan prospects into A-1 credit risks.

This particular data bank, called TRW Credit Data, is operated by a unit of Cleveland's TRW Inc. It is the biggest service providing information to subscriber businesses granting consumer credit—banks, finance companies, oil companies and large merchants.

As such, it has become a juicy target for con artists who are giving a new technological twist to the credit-fraud game. But TRW Credit Data isn't alone. Many credit-reporting services, including other large data banks, are being victimized with a frequency that suggests a growing crime wave.

NATIONWIDE SCOPE

Total losses to businesses making loans on the basis of falsified credit reports aren't known but probably are huge. If there is a foolproof defense against such swindles, it obviously hasn't been found.

Risk of such losses has grown with the prevalence of credit use and the centralization of the credit-reporting industry into a handful of computerized giants who now dominate it. Local and regional credit bureaus still exist, but big grantors of credit rely more and more heavily on the big national data banks.

Almost every kind of credit transaction an individual enters into with a business subscribing to a data bank is fed into that bank. In turn, the data bank makes all the information it has on a person immediately available to any subscriber who asks for it. The speed, capacity and nationwide scope of the data banks have led some subscribers to cut back or even eliminate their own checking of a credit applicant's references. This means that establishing false credit in a single national data bank like TRW's can be enough to set up a sizable swindle.

"The striking thing is the ease with which this can be done," says a federal prosecutor who is digging into one such case. "It demonstrates an enormous potential for fraud. With access to a national system, you can commit any number of frauds in any location across the country. The customers of these data banks are completely exposed because they lean so heavily on those computer reports."

SOME INSIDE JOBS

Taking advantage of this, enterprising crooks are subverting the data banks in a number of ways. Some set up fictitious businesses that subscribe to the data services with the sole purpose of then pumping into the computer bogus transactions that establish bogus credit records in the data bank. Others use crooked employees at legitimate subscriber businesses to do the same thing. And some have been able to use employees at the data banks themselves, inducing them to file bogus information directly into the computers. The crooks then tap the artificially created credit themselves or peddle clean credit records to others.

Even a single operator can net a huge haul, as the case of John L. Spillane, an engineer from New Jersey, clearly shows. He set up fictitious companies and used them to obtain bank loans and to pump false information into data banks to which one business subscribed. He used roughly 300 aliases, and saw to it that all had spotless credit standings.

From 1970 to 1974 he drained \$660,000 in loans, goods and services from banks and businesses in several Eastern states. During this span, he was issued about 1,000 credit and charge cards in various names. Finally caught, he pleaded guilty to federal fraud charges in December and now awaits sentencing in federal court in Camden, N.J.

Lone-wolf operators of his ability and industry are comfortingly rare. Law enforcers are more concerned about the increasing role of well-organized rings that have the manpower and patience to pull off potentially enormous swindles. The sale of clean credit by these rings, an important part of some such operations, leads federal investigators to suspect that some may be tied to organized crime.

"ORGANIZATION" IMPLICATION

"The organization is ideally suited to this," a federal investigator says. "They have the network, the connections, to seek out and find the kind of people who need fixed or false credit, and they've got the expertise to recruit insiders, too."

The sale of credit can be an extremely lucrative business, says Spencer Nilson, a credit expert and publisher of a credit-card industry newsletter, the Nilson Report. "Regardless of who or what you are, if you know where to go in Los Angeles, you can buy an unblemished record within two weeks for \$500," he declares. Besides the essential clean rating in a national data bank, a deluxe package might also include credit cards, a bogus driver's license, a choice of ID cards and even a passport—presumably enabling the holder to skip the country after he has made his score, Mr. Nilson says.

The extent of penetrations into the national data banks isn't clear, but cases of dishonest data-bank employees falsifying credit information for accomplices on the outside have been confirmed by TRW, Equifax Corp. of Atlanta (formerly Retail Credit Co.) and Trans Union Corp. of Chicago. Some operations that have come to light indicate how difficult it is to combat or even find a well-organized ring.

In 1971, according to police and bank investigators, a group known as the Turner-Curtis gang recruited insiders at TRW Credit Data and Trans Union's Computer Credit Corp. to establish false identities and credit records in the companies' computers. The gang also hedged its bets by placing its people in credit positions at some 20 banks, finance companies, and retail businesses; their job was to feed false information into the data banks to which their employers subscribed and to assemble physical files that would back up the computers' data.

In this setup, even an unusually cautious subscriber business, desiring more than a TRW or Computer Credit Corp. report before extending credit, could call an applicant's references directly—and find there a file matching the computer information. Besides using the bogus credit themselves, the gang sold fake references at \$50 each to outsiders. A single victim of the fraud, the Newport National Bank of Newport Beach, Calif., lost \$200,000 in loans made on cars that didn't exist to borrowers who turned out to be bogus.

One ringleader, James Curtis, pleaded guilty in 1971 to charges of making false financial statements. He was placed on probation and fined \$1,000 in a state court in Orange County. Edward Turner, who police say is the other ringleader, is still a fugitive from a warrant arising out of the credit-fraud case.

TRW says it hasn't any knowledge of insiders at its Los Angeles offices who worked for the Turner-Curtis gang in 1971. Computer Credit Corp., a unit of Trans Union, confirms that the ring placed an insider at its data bank.

The so-called Harris gang, operating in 1973 and 1974, planted its members in even more legitimate businesses. It used a phony business school specializing in credit procedures as a front. The "graduates" had little difficulty in finding jobs at businesses subscribing to TRW Credit Data, such as Sears, Roebuck & Co., California Federal Savings & Loan, Beneficial Finance and Crocker National Bank, according to police.

Using and selling credit, the ring's operations drained an unknown amount—up to \$1 million from banks and finance companies alone, it is estimated—from businesses in Los Angeles, Orange and San Diego Counties. Even the most cautious were victimized.

Mobile Services Consultants of Orange, Calif., for example, didn't satisfy itself with just the TRW report on an applicant for an \$8,000 recreational-vehicle loan. The bonded credit facilitator for banks took the added precaution of calling all the applicant's references.

The applicant got a clean rating from each, and he also got his bank loan. But when the payment book bounced back to the bank marked "addressee unknown," and Mobile Services rechecked the references, the files had all been removed.

Paul Budnovitch, a vice president at Lloyds Bank, another victim, says there isn't a really effective defense for lenders against such a double-pronged scheme. "If you get a clean TRW report, the application looks easy to accept," he says, "and if you then have a retailer pull a file and they give you the right answers—well, you can't reasonably suspect there's anything wrong."

The Harris gang was finally halted when an undercover agent arranged for a purchase of credit credentials and led police to the home of ringleader James Harris, who was caught with 300 credit-reporting forms of TRW, filled with phony information and ready to be filed. Harris, who had a previous police record, pleaded no contest last July to charges of making false financial statements and was placed on two years probation by a state court in Santa Ana.

If credit grantors careful enough to call references themselves can be defrauded, less careful ones are pushovers. A number of Detroit banks learned this to their sorrow last year when con men made off with the proceeds of numerous loans made on the basis of bogus TRW reports. The only other checking done by the banks themselves was to call the phone numbers given by the loan applicants for their places of work.

The places of work turned out to be fictitious. The telephones were all located in one room and apparently manned by the ring members, who eagerly verified that, yes, the applicant did indeed work for the company. "We were pretty damn lax, I have to admit," says one burned banker. He says the faked TRW reports looked like an inside job. TRW Credit Data declines to comment on the case. There are at least 70 suspects but no arrests as the FBI and postal authorities continue their investigation.

Meanwhile, a federal grand jury in Los Angeles is investigating the activities of still another ring that penetrated TRW Credit Data in late 1974 and early 1975 by recruiting an insider, a computer-terminal operator whom the company says it will prosecute. The ring apparently fleeced businesses in Southern California, Las Vegas and possibly elsewhere, sources say.

Although TRW Credit Data's position as the largest supplier of consumer-credit references makes it a favorite target for fraud, other major data banks such as Equifax and Trans Union are victimized too. Police say TRW has an able security force and a good security system, but some schemes are difficult to detect until it is too late.

Edward J. Brennan, Jr., vice president and general manager of TRW Information Services, the TRW subsidiary that operates the Anaheim-data bank, says no security system can completely protect TRW Credit Data or its subscribers from a dishonest employee at the data bank itself, or from ring members planted inside legitimate subscriber businesses.

TRW has, however, taken steps for more careful screening of subscriber companies to try to prevent false information from being fed into its computers. It acted after it discovered last year that a con artist had established six phony identities with clean credit by inserting bogus transactions for them through subscriber companies that turned out to be fictitious.

Mr. Brennan argues, however, that the frauds uncovered at TRW Credit Data are insignificant when compared to the enormous volume of credit transactions handled by the concern. "The banks haven't communicated any great concern," he says.

Most TRW Credit Data subscribers seem to be understanding about the knotty problems of security. But at least three subscribers, including a large nationwide finance company that relies heavily on TRW, expressed doubts about whether the company is doing everything possible to help them protect themselves from fraud.

The total cost to business of data-bank fraud, as well as other varieties of credit fraud, may never be known. The victims themselves are often so sloppy in their own procedures that huge amounts of fraud losses are unwittingly written off as simple bad debts, credit investigators say. Other businesses that know they have been stung keep their mouths shut for fear publicity will embarrass them or encourage other crooks to get into the game.

Some Detroit banks listed as victims of the data bank ring there by authorities investigating the case profess ignorance of it when questioned by a reporter. The vice chairman of a major West Coast bank victimized by one ring, when told of inquiries about credit fraud, angrily told subordinates to stonewall on the entire subject.

Moreover, credit lenders generally don't bother to report suspected fraud to the police because there seems to be little chance that the perpetrators will be caught and effectively punished anyway. Many police forces pay almost no attention to credit fraud; in Boston, only one detective is assigned to credit-card and check fraud. "It's crazy," says Fred Thompson, the beleaguered man in charge. Though authorities say Los Angeles is a hotspot of credit fraud, only a single two-man team works the false-documents beat.

Legal difficulties abound too. Lacking concrete proof of fraud, that the businesses have no more than a civil complaint against a deadbeat. Investigators say they are hampered by fair-credit reporting laws that forbid or restrict credit lenders sharing of information with each other.

Prosecutors say that to sustain a criminal case they must be prepared to prove that fraud was actually intended, and this is often difficult. As the Turner-Curtis and Harris cases indicate, the perpetrators often escape any prison sentences.

(Equifax actually declined to prosecute its suspected insider, a terminal operator who allegedly falsified data in 1975 for a gang engaged in doctoring the credit reports of poor risks. Although the ring leader, William B. Givins, pleaded guilty to a felony fraud charge and received probation, Equifax said it wasn't interested in charging the terminal operator because prosecution was so difficult and it considered her firing sanction enough.)

The potential rewards and the seeming ease of escaping any heavy punishment have made credit fraud an enormous secret industry, ac-

ording to Mr. Nilson of the Nilson Report. He estimates that frauds involving credit cards alone last year cost businesses more than \$500 million.

A pilot project done by Hooper-Holmes Bureau Inc., a New Jersey-based credit reporting service, offers some support for Mr. Nilson's alarm. From April through June of 1975, Hooper-Holmes took credit applications submitted to it by nine big credit grantors—including Diners Club, Carte Blanche and several major oil companies—and compared them against its own "small" master list of 250,000 names and addresses culled from applications previously detected as fraudulent.

Hooper-Holmes found that almost 20% of the applications passed on by the credit-card and oil companies were linked to certain indicators of fraud. (In a related study, the credit bureau found that 181 applications came from one address, which turned out to be a vacant building in Minneapolis.) During the 90-day test, Hooper-Holmes doubled the size of its suspect file.

[From the Wall Street Journal, Mar. 22, 1971]

SABOTAGE, ACCIDENTS AND FRAUD CAUSE WOES FOR COMPUTER CENTERS

(By A. Richard Immel)

One crisp winter weekend a little over a year ago, five members of an antiwar group called Beaver 55 broke into Dow Chemical Corp.'s Midland, Mich., data research computer center and ransacked the place.

"Tapes and cards were thrown all over the floor," a Dow Chemical official recalls, "but damage appeared to be slight." That is, until someone in the clean-up crew discovered a small, circular magnet about the size of a quarter in the debris. The following Monday, when the computer tapes were checked out, the manager of the center discovered to his horror that the data on 1,000 of the tapes has been erased by such magnets. Cost to reconstruct it: \$100,000.

Computer center operators are finding out the hard way that the Dow incident wasn't an isolated occurrence. Last year millions of dollars worth of computer equipment and data were damaged and destroyed by sabotage alone. Add to that increasing instances of computer misuse—such as for fraud and embezzlement—and serious accidental disruptions, and it becomes clear why some observers see troubles ahead in the computer age.

BUTTONING UP THE COMPUTERS

The growing specter of deliberate and accidental assaults on computers has spawned a new kind of consulting firm that tells companies how to button up their computer operations to avoid embarrassing—and usually costly—incidents. Within the past two years, about a dozen of these computer-policing concerns have appeared, offering everything from a simple security checkup to the complete rebuilding of a company's computer center.

Lou Scoma, an Illinois computer-security expert who heads two-year-old Data Processing Security Inc., sees a wide-open market for his services. He projects revenue of \$4 million this year, up from \$300,000 in 1970, and expects to draw heavily from the 90% of the nation's 70,000 computer centers that he considers to have inadequate security.

Joe Wasserman, another pioneer in the field, says: "Computer security in general stinks. Computer centers tend to be either completely secure or completely insecure." He says most of the secure ones are companies dealing with classified government work—"and that's a pretty small number." Mr. Wasserman expects his New Jersey firm, Computer Audit-Systems Inc., to do five times the business it did last year.

Many companies, of course, have long had their own security experts who were responsible for protecting company property and trade secrets. In recent times sabotage by antiwar groups or other members of the "anticomputer culture" has become a major concern of such security departments. A number of security executives employed by Western U.S. companies with large stakes in research and development have formed a group called Research Security Associates, which meets quarterly to swap information on sabotage threats and techniques and the people thought to be responsible for them. But security experts admit this type of watchfulness is only partly effective. "The biggest problem with the anticomputer culture is that it isn't organized. You can't develop data on them," complains one security man.

FROM SHOPLIFTING TO BOMBS

It isn't just war-related industries that are being threatened. "Seven years ago we were worried about shoplifting and employee theft," says the security chief for a national grocery chain, "Now it's bomb threats and computers." Bewildered executives of one West Coast clothing manufacturer got eight bomb threats against their computer last year.

Sometimes the danger comes from within. A computer employee at one company was given two weeks' notice before he was laid off. The man promptly removed all the labels on 1,500 reels of tape, costing the company thousands of dollars in labor to reidentify the data. "The people I talk to are beginning to realize that things can happen to them that just don't make sense," says one consultant.

As Dow Chemical found out, the technology of computer disruption is ridiculously simple and widely known. Last June a Chicago underground newspaper called Seed published explicit directions on how to wreck computers and erase tapes.

The advice didn't stop with breaking and entering. The article counseled would-be saboteurs to join the institutions they want to sabotage as computer operators and programmers and work from within.

INADEQUATE BUT DAMAGING

Instructions similar to those in Seed have appeared in a number of other underground publications as well.

In some cases the disruption can be inadvertent, but it's no less damaging. One West Coast data processing manager lost his job when

a group of Boy Scouts touring the computer center happened to have some magnets with them that erased most of the company's records stored on tapes. In another case a repairman stuck his magnetic flashlight to the nearest support—which happened to be a data storage drum. The result: 80,000 scrambled customer credit records.

A less dramatic but potentially costly security problem is theft or embezzlement by computer personnel. Last summer, for example, Encyclopaedia Britannica accused three operators on the night shift of copying nearly three million names from the company's "most valued" customer list and selling them to a direct-mail advertiser. Britannica has sued the employees for \$4 million, claiming \$3 million of the amount in actual damages.

Security experts say many companies probably are losing large sums each year without even realizing it. Brandt Allen, an associate professor in the University of Virginia graduate school of business, says the airlines industry alone may be losing as much as \$1 million.

What bothers many is the simplicity of the fraud and embezzlement schemes that have come to light so far. "One can't help but wonder what the really clever people are doing," says Mr. Allen.

The same thoughts are haunting some members of the accounting profession. Jerome Farmer, chairman of a computer committee of the American Institute of Certified Public Accountants, concedes that manipulation of computerized records could escape the attention of auditors. But he says accountants are working to come up with techniques to overcome the problem.

STEALING BY TELEPHONE

One potentially vulnerable type of computer is the "time-sharing" unit used by many customers. It's possible to steal data from such a computer by telephone.

Last summer, for example, the FBI charged a teen-ager with stealing information from a time-sharing computer system in Louisville by long-distance phone. After obtaining account and password numbers of system customers, the youth allegedly tapped into the computer by calling in from Cincinnati. According to the FBI report, he had nearly worked out a program to permanently bypass the center's security safeguards when a mistake tipped his hand.

Two weeks ago, in a similar case, Information Systems Design, an Oakland, Calif., computer service firm, filed a \$6 million civil damage suit against University Computing Co. of Dallas, charging two University Computing employees with stealing computer programs by long-distance telephone. The civil suit followed a criminal charge of grand theft against one of the pair. The suspect has pleaded innocent.

NO MORE FISHBOWLS

For those seeking ways to guard against sabotage or other damage to computer systems, one obvious step is to improve the guarding of data processing installations. Many companies and institutions have been so proud of their big, expensive computers that they have put them on public display, enclosing them in "fishbowl" glass cages and including them on guided tours. But many firms now are quietly cut-

ting back or discontinuing such tours, and the old glass walls are giving way to reinforced concrete.

Companies also are being more circumspect about acknowledging that they even use computers and about advertising their location. In San Francisco, for example, several big banks have removed all bank identification from the buildings that house their computer centers, and in Chicago a large retail concern has changed its computer print-outs to make them look typewritten. "When it comes to data processing operations, we would prefer that people didn't even know we had computers," a spokesman is quoted anonymously in a trade journal.

Those companies that seek outside help in improving the security of their computer systems find that prices start relatively low, but they can quickly escalate to astronomical levels. Mr. Scoma of Data Processing Security will put a team of consultants to work running through a 172-point checklist and preparing a survey report for \$3,000 to \$5,000. The report points out security weaknesses, estimates the cost to reconstruct lost or destroyed data and recommends procedures and equipment to plug any gaps.

STEEPLY RISING COSTS

The plugging is the expensive part. Mr. Scoma offers a package that includes a double-door "buffer" system with electric locks, magnet sensors and closed-circuit television to control access to computer centers. The cost: \$25,000. Backup power systems, which can be critical where computers can't be permitted to shut down during a power failure, may run anywhere from \$50,000 for a simple generator to upwards of \$1 million for the systems used by airlines for their computerized ticket reservations.

Some consultants say at least part of the blame for the vulnerability of computers lies with computer manufacturers that have failed to build security measures into their systems. A spokesman for IBM, the nation's largest computer maker, refuses to talk about the matter, protesting that "we don't feel that publicizing (the security problem) is in our best interest." But Honeywell Inc., which bills itself as second only to IBM in computer sales, concedes that more could be done.

John Weil, who heads Honeywell's advanced systems and technology unit, says the industry has tended to neglect the security problem in its haste to develop basic computer technology. But he says Honeywell, for one, now is working on protective equipment and techniques, though he says they will have to be built into its systems from the ground up. "I think it will take the next generation of equipment to introduce these things into the basic equipment," he says—and that is several years away at least.

[From Menkus on Management Newsletter, August 1972]

COMPUTERIZED INFORMATION SYSTEMS ARE VULNERABLE TO FRAUD AND EMBEZZLEMENT

(By Belden Menkus)¹

There is no such thing as a *fraud proof* or *embezzlement proof* information system. This confirmed by a statement in the 14 June 1971

¹ Belden Menkus is a consultant serving with the Computer Security Institute.

Security Letter by Marshall Armstrong, president of the American Institute of Certified Public Accountants. He said, "No accountant in the history of our profession has been able to establish foolproof controls against fraud and embezzlement . . . creating foolproof controls is impossible." Because people design and use an information system, it is plainly impossible for someone to design a system that someone else cannot compromise or manipulate. This is equally true with computerized information systems. In 25 June 1971 testimony before the Senate Permanent Investigations Subcommittee John Beardsley, Hartford Insurance Group Vice-President, said that "After 30 years in this business I am absolutely sure there will be ways found to steal via computer." Mr. Beardsley could have added that people already *are stealing* by computer.

There is nothing inherently *secure* about the physical nature of a computer or the way in which it processes information. The basic concept of a computer's function may be stated this way: It is a complex of machines that can compare and add or subtract discrete units of information and maintain a running tally of what it has done. The computer can do this very fast and with exceptional accuracy. Advances in data processing technology have increased the amount of information that the computer can handle at any given time and expanded the number of different ways in which its simple capabilities can be used. However, the essential nature of the computer has not changed: It still cannot rationally analyze the tasks that it performs or the nature of the information that it works with. The computer can perform the same task repeatedly with little or no operational error, but it is not capable of a creative thought. Someone must think *for* the computer; it is at this point that the vulnerability of computerized information processing systems first is exposed. The work done by the computer will be no more reliable than is the information it is given to work with.

The computer will check data presented to it before accepting the data item for storage or processing. The machine routines that do this, however, are designed to verify the validity of the data, not its *integrity*. But as Dr. Jan Polissar notes in *Modern Data* for May 1971: "Some types of data just cannot be checked by the computer. The systems depends on the operator checking what he enters." Checks for bit parity error, field lengths and similar factors are intended to assure that the data items meet the logical requirements of the system. These checks determine that the information is in a form suitable for processing and that its code structure and other inherent features meet the specifications of the computer program being used to process it. No effort is made to determine if the information itself is authentic. If, for example, the *customer name* entry is no longer than the space allowed for it, or the number of units involved in the transaction is not excessive, the data item will be accepted for processing even if the transaction that it represents is fraudulent.

John Mason and William Connelly, writing in the September-October 1971 *Management Adviser*, observe that "self-checking digit methods [commonly used for data entry control] are capable of generating check digits which have but ten possible values, 0 through 9. Because

more than one code number will be assigned the same check digit, there is always the possibility that a substitution or transposition of digits in one number may result in another valid number (the latter number having the same check digit as the former number)."

Converting an existing information system from manual processing to an electronic data processing system does not of itself assure the *security* of the information system. In fact, through this transformation the system and the information that it is used to process may become more vulnerable to compromise.

Manual information systems are error-prone and subject to some manipulation, but their very nature provides some control features lacking in computerized systems. Manual systems rely on documents that can be counted, traced through system processing steps and independently verified. (Batch processing computer based information systems provided some of these operating features, but these have largely disappeared with the development of more advanced computer systems.) Manual data transmission creates certain admittedly redundant operating checks and encourages separation of duties in a way that limits individual access to the processing of the entire transaction. Concentration of data in a computer facility removes these manual system safeguards. And, paradoxically, the greater access to the information provided by remote terminal access devices makes this information more vulnerable to possible compromise.

Certain features inherent in computer systems operations make it easier to compromise the data being processed. These include: (a) handling data in a form suitable for machine processing but that cannot be read by people; (b) limiting the number of people handling data but expanding their access to it and their ability to influence processing of particular transactions; and (c) eliminating intermediate records and processing summaries, which makes it difficult—if not impractical—to independently examine or verify data processing activities.

Frauds in computerized information systems may be perpetrated in four different ways:

1. Transactions direct with employees. (As in brokerage house employee margin accounts, discretionary purchase accounts, and travel expenses *funds*.)

2. Transactions falsely entered with non-existent persons or companies. (These basically are manipulations of customer invoicing accounts payable functions. However, the chairman of a national securities brokerage firm is reported to be particularly concerned with the possible loss of integrity in customer accounts. They can be opened directly by branch office registered reps and accepted by the central data processing system without home office review.)

3. Transaction with employee accomplices in other companies. (A form of simple collusion.)

4. Transactions instigated by third parties. (In most instances this involves bribery or intimidation of employees to force them to commit fraud.)

Every compromise of the data in a computerized system does not result from fraud. Some problems are created through honest employee errors. For instance, errors may be made in the data capture

process. Or, the computer machine operator may mount a master customer file tape where a transaction tape should be placed and write over the master file, effectively destroying the data on it. Or, the programmer may fail to properly check or *debug* a program before it is put into use. Logical or operational errors in the program and its use by the computer may persist undetected for months. And, these errors may leave little or no evidence that they are the cause of faulty transaction or master file records. Too, it must be recognized that errors made in computerized information systems have a cumulative effect on future transactions and on related processing activities that is unknown in the operation of a manual information system.

There are two main aspects to computer system vulnerability to fraud and embezzlement.

(a) *Inadequate or irregular computer program and master file maintenance.* This may involve alteration of the program to give special unauthorized or irregular treatment to particular transaction types or to the files of a particular customer. (One example of what this can mean is a delinquent account file that was designed by the programmer to fail to record nonpayment of accounts by certain individuals.) This may also involve improperly made—but properly authorized—file and program modifications.

(b) *Data, program or master file manipulation during transaction origination, transmission and processing.* The possibilities seem to be limited only by the ingenuity of the people involved. For instance, false data can be introduced into the transaction. Or, valid data can be destroyed or modified. Remote data access and transmission capabilities make it possible to do this undetected from a distance. The dynamic environment in which so-called *real time* systems operate tends to destroy data as it is superseded by later information. This type of advanced design computerized information system is vulnerable to functional errors that can destroy segments of files and transaction records. This same condition of *operational flux* makes data lateration easier to accomplish and more difficult to detect.

[From the Computerworld, May 10, 1976]

ERROR RATE FOR SSI CHECKS HIT 23.7%

(By Edith Holmes)

WASHINGTON, D.C.—Almost one-quarter of the computer-generated checks sent to recipients of the Social Security Administration's (SSA) newest federal welfare program in the last half of 1975 were wrong, the agency's Quality Assurance Program has determined.

The latest statistics for the SSA's two-year-old program for blind, aged and disabled adults showed a 23.7% error rate in payments made to a sample of the 4.3 million people covered under Supplemental Security Income (SSI).

With the study 99% complete, this error rate matched rather than improved upon the record of the SSI system in its earlier stages, despite expectations for improvement by the end of last year, according to SSA Commissioner James B. Cardwell.

Cardwell told the House Ways and Means Oversight Subcommittee chaired by Rep. Charles A. Vanik (D-Ohio) here recently that he and others in SSA anticipated an improvement in SSI's error rate because a computerized hookup to the regular Social Security benefits of clients, designed to check clients' real needs and reduce their benefits accordingly, became operational during this period.

SSI's interface with the rest of the benefits offered by SSA programs may actually account for an improvement in the error rate, but "there may be something that is offsetting it," Cardwell said before the committee currently investigating SSI.

COMMISSIONER PUZZLED

The commissioner indicated he was puzzled by the only "marginally lower" error rate. Some of the errors—up to 40% of them—were due to "client behavior" and will probably continue to be present in this national attempt, begun Jan. 1, 1974, to simplify and improve on state, county and city efforts to provide welfare for adults, he suggested.

The balance of the SSI errors could still be attributable to SSA's elaborate computer system, under study by various congressional committees—including Vanik's oversight committee and the House Government Operations Subcommittee, chaired by Rep. L. H. Fountain (D-N.C.), which commissioned the General Accounting Office (GAO) audit of the SSA's computer operations now in preliminary report form [CW, April 26].

Quality Assurance figures for July 1 to Dec. 31, 1975 showed the 23.7% error rate breaks down to 9.8% in SSI overpayments, 7.8% in ineligible payments and 6.1% in underpayments to recipients.

The overall error rate for the last six months of 1974 was 24.8%; for the first six months of 1975, it was 24.4%, according to the SSA program's numbers.

Cardwell and other agency heads expected that figure to drop to 19% or less once the computerized records of people who receive regular Social Security benefits were linked to SSI records. Because of eleventh-hour changes in the SSI program by Congress and management problems in SSA, the Bureau of Supplemental Security Income and the Bureau of Data Processing, both within the SSA, were unable to connect the files for these separate payment systems until early last summer.

The agency has also recently discovered several SSI clients have undisclosed bank accounts that can make them ineligible for supplemental income, he said.

This may be primarily a "training problem," he added, which can be solved by teaching agency caseworkers to ask the right questions during initial interviews to determine client eligibility.

Vanik pressed Cardwell about numerous studies of the SSA's computer operations conducted since 1971, focusing particularly on the recently completed but as yet unannounced GAO audit.

That report indicates SSA computer utilization is only 50%, the congressman said; a committee staff observer later stated Vanik was being generous.

EXPECTS GAO REVISION

Cardwell, who has stated the computer operation at SSA is in need of a complete overhaul to the tune of some \$500 million, told the committee he takes issue with the GAO audit report—a “very quick analysis” disputed by other computer experts.

The GAO may be revising its estimate that the SSA uses only 40% of the capacity of its 17 large-scale computers, he said.

SSA needs new computer technology and facilities because in a few years the 34 million checks it now processes each month will reach 50 million, Cardwell stated.

The commissioner characterized the SSA’s computer operation as “a patchwork” put together over the last 10 to 15 years under congressional mandates to meet the needs of increasing numbers of welfare programs.

While “it may be that we put some patches where they were not necessary,” Cardwell said he feared the risks of “a breakdown of service” without the proposed expenditures for the computer operation.

With the new technology, which the agency estimates would be installed over a period of five years SSA might “leap-frog” to a system that bypasses “both check writing and the post office,” Cardwell said.

But while he contended “we’re just passing too much paper around,” Cardwell suggested welfare recipients are often wary of banks and so might react negatively to an electronic funds transfer system. He thought any such system should first be tested on federal employees.

[From the Nation’s Business, April 1971]

GUARD THAT COMPUTER

An underground Chicago newspaper named *Seed* recently turned its attention to computers.

In the past, it said, “a group of extremists called Luddites smashed machines because they felt them to be the work of the devil.”

Today, it added, some feel the same way about computers. For its readers who do, it offered a full-length how-to-do-it article on “The Technology of Computer Destruction.”

“Unfortunately,” notes Robert V. Jacobson, president of Bradford Associates, Inc., of New York, consultants on computer security, “about 80 per cent of what that article says is true.

“Once, human error was the most dangerous threat to a company’s computer center. Today, it’s sabotage.”

Sabotage has become a familiar, ugly, part of the American scene.

The FBI reports actual and attempted bombings now run at the rate of 433 a month. The bombers’ handiwork is witnessed on the campus, at government buildings including the U.S. Capitol itself, and, of course at businesses.

And the radical left is clearly beginning to look on the computer center—in the corporations and on the campus—as a prime target.

“We got four bomb threats one day,” says the security officer of a big Manhattan bank. “One was directed at the computer center.”

Last fall, at an SDS "convocation of youth" in Milwaukee, a latter-day La Passionara told the audience that computers are to modern man what the Spanish Inquisition was to "those of yesterday who sought only to escape the tyranny of a cruel religion."

Computers, she said, are just "malicious gossipers tattling untruths to eager ears."

The young firebrand, who called herself Delilah, urged that electronic data centers be sabotaged because they "pinion free men to the display board of a sick and greedy society."

MANY ARE OFF GUARD

Despite this sort of thing, Mr. Jacobson says, "I find a surprising number of men in top management, very prudent otherwise, who are astonishingly indifferent to what should be a major concern of theirs. Namely, what would happen to their corporation if its computer center were knocked out or its tape library destroyed.

"The crux of the problem is this. Computers have grown immensely in technical capability. From mere tombstone accounting—telling us what happened last week—they have now become part of the company's daily operation.

"They're as much a part of it as the machine tool on the factory floor."

How serious would destruction of a computer center be?

"The computer itself would be easiest to replace," says Louis Scoma Jr., president of Data Processing Security, Inc., Hinsdale, Ill.

"The manufacturer would do his utmost to rush a replacement quickly. But the software—the company's records, and the programs that tell the computer how to process them—may be almost irreplaceable."

Unfortunately, they are also most vulnerable.

"A strong magnet, the kind you can buy at any hardware store," Mr. Scoma says, "can play havoc with computer tape. You can ruin 1,000 reels in 15 minutes by holding a magnet close to them and walking through the tape library."

That magnetic force scrambles the billions of bits of information on the tapes and makes them useless.

Computer security officers recite examples galore of planned or accidental destruction.

One night in December, 1969, members of a radical antiwar group calling itself Beaver 55 broke into a Dow Chemical Co. data center in Midland, Mich. They climbed a fence, forced a locked door to the tape library, then left after a few busy minutes.

The next morning, Dow employees found the place "a mess," but apparently little harmed.

"They scattered a few tapes and some IBM cards over the floor," a company spokesman says. "It looked like minor damage only."

But closer examination told a different story.

"They ran a magnet over about 1,000 tapes and wrecked 'em," the spokesman says.

Beaver 55 boasted that it had destroyed data from "research into such areas as nerve gases, napalm, defoliants and other secret chemical weapons."

Actually, it had erased—along with tapes that held the records of the local blood bank, research on air pollution, and the history of Dow's industrial health program—the chemical test results of a mumps vaccine Dow was developing.

Dow had duplicate tapes for some of those destroyed, and backup data for all. But it was a costly and time-consuming job to reassemble the records. The company estimates damages at \$100,000.

DANGER: GRUDGE AT WORK

A disgruntled worker can be as dangerous as a campus radical.

One Midwestern firm was brought to the brink of bankruptcy, computer security officers say, by a programmer with a grudge.

He was fired in the morning and came back after lunch to clean out his desk. During his lunch hour, he had bought a magnet.

His boss had failed to tell other computer center employees that their colleague had been dismissed. So he had no trouble entering the center and its tape library. In 10 or 15 minutes, he erased virtually all the company's files and computer programs.

Among vital records that vanished were the company's general ledger accounting system, its accounts receivable and accounts payable, all stockholder records and valuable marketing data.

Management found, to its dismay, that it had little backup information on tape or on paper.

It began a laborious effort to reconstruct its records with the help of its auditor and other sources.

But its survival was touch and go.

"Here's what a situation like that would be like," says Brandt Allen, associate professor at the Graduate School of Business Administration, University of Virginia, and a consultant on computer security systems.

"The company couldn't send out bills. It wouldn't know who owed it, or how much. It couldn't pay bills—for the same reasons.

"And it couldn't refuse to pay a bill, if presented, even if it doubted that the goods or services had been delivered. It would have no written record to dispute the claim.

"Furthermore, it would have great difficulty running its plants.

"Today, many companies use the computer to run off their daily production schedules. The computer takes into consideration the backlog to be filled, the items on order, what work was done last night, where partly-finished items are on the factory floor and in what stage of manufacture they're in, and what production runs have priority.

"It also remembers what machines are available, what supplies are on hand and where the materials are. It figures out how long each job will take, what to do if slippages occur.

"It may provide eight or nine alternatives to take if the plant runs into production snags.

"Often, the computer will lay out an over-all schedule, leaving the fine tuning to plant managers.

"Then, every morning before they get to work, the computer will have typed a print-out of their duties for the day for top management, superintendents and foremen. It may send 1,000 print-outs daily to 1,000 different people.

"The people who run the plant simply wouldn't know where to start without the computer."

ERROR IS A TERROR

To protect it properly requires more than just a list of things to do before the bomb squad comes, says Joseph Wasserman, president, Computer Audit Systems, Inc., East Orange, N.J.

"A good security system must anticipate trouble," he adds. "And it must protect against human error as well as human malice."

To their regret, human error is what these companies failed to guard against:

One manufacturer found that some data stored in its center's memory drums had been wiped out completely. Unluckily, it had no duplicate of the information on tape—or elsewhere. Working from other hastily assembled records, it was finally able to piece the information together.

Meanwhile, its computer was shut down for six days.

The cause: An employee who was cleaning the inside of the drum cabinet had attached his magnetic flashlight to the unit.

At a company computer center in Louisville, Ky., maintenance costs went sky-high following every local thunderstorm. For as long as a month afterward, components conked out mysteriously, shutting down the computer.

The cause: Lack of proper shielding from the electrical energy generated by lightning bolts.

A big Eastern bank found serious and recurring errors in its payroll records and lists of depositors' account numbers.

The cause: A magnetic door-opener at the entrance to the tape library. As tapes were hauled past in a cart, the gadget erased the data on the side of the tape nearest to it.

"Even airport radar can be a danger," says Henry Hoffart, a San Diego consultant on electromagnetic compatibility and an authority on grounding systems.

"The beam can erase tapes or induce a current in the computer circuitry. This can badly distort the information you are trying to store on your tapes, without so much as a hint that anything's amiss.

"The programmer thinks the input is O.K.—then plays it back and finds it unreadable."

UNPLEASANT VISITS

As more of top management decides that the computer center is its most vital and most vulnerable physical asset, guided tours of that installation are less and less likely.

A large insurance company discovered the hard way why such tours may be good community relations—but bad corporate policy.

Not long ago, a ladies' garden club accepted an invitation to visit the company's new computer center.

One lady was fascinated by the blinking lights, the whirring tapes, and the general Buck Rogers atmosphere of this space age hardware. In fact, she was so impressed that she felt impelled to take home a souvenir.

"I meant no harm," she said later. "But there were all these trays of punch cards lying on a table, so I reached into a tray and took one."

The cards were "program patches," used to put new steps or procedures into a taped computer program.

The data processing department, of course, was not aware that one of its cards was missing. As a result, when it ran them through, and the "patched" program refused to work, it was baffled.

It took a week of costly, agonizing sleuthing to discover what had happened.

"Business is learning that the computer center isn't a showplace," says Harold Weiss, director of the Automation Training Center, Reston, Va. "It's the corporate nerve center. It must be protected, just as nature protects our brain with a massive bone structure.

"Putting it behind plate glass, like a department store window, is like putting an isinglass peephole in your skull."

Mr. Scoma, at an American Management Association seminar on computer security, asked: "How many banks put their vaults in their front windows? How many financial institutions let visitors wander through their safe deposit box areas?"

TAKING PRECAUTIONS

Mr. Scoma's firm specializes in security systems for data processing centers. It has designed and installed more than 100. They include TV monitors, coded ID cards and other hardware to guard against theft, vandalism, sabotage, riot or fire.

St. Paul Fire and Marine Insurance Co., the first to offer special insurance protection for computer installations, says a long list of factors enters into its determination of risk.

Here are some main points it checks:

Location.—What type of building the center is in, and where the computer is located in the center. The computer should be, if possible, in an inside area with few or no windows, and not on an outside wall. It should not be in the basement because of danger of water damage.

Fire Protection.—Is the center equipped with sprinklers, Halon 1301 or carbon dioxide extinguishing systems? Are combustible materials stored near it?

Air-Conditioning.—Does it have an auxiliary air-conditioning system that can be used if the building equipment fails? Does it have backup power and water supply?

Security.—Is there an effective system to make sure that only those who have a need to do so are admitted to the center or the tape library?

Disaster Plan.—Is there a written procedure for evacuation of the center in case of emergency, and for protection of its contents?

Record Protection.—Is there a system for insuring that duplicate master tapes, program tapes and transaction tapes are made and kept in a separate, fireproof location?

Housekeeping.—Are all activities which might endanger the center performed away from it? For example, repairs which involve soldering or welding.

Environment.—Is the center's location one where riots are unlikely?

"We stress that the No. 1 thing is to protect the data processing center and its tape library as best you can," says Gordon Paine, assistant secretary of St. Paul Fire and Marine.

“They’re vital installations. Without them, the company is a dead duck.”

[From The Washington Post, May 23, 1976]

DIVORCING BY COMPUTER?

(By Kathryn Christensen)

CHICAGO—For nearly 11,000 women in Cook County (Chicago and suburbs), the first step in divorcing their husbands in the last two years has been to tell their marital problems to a computer.

Though the computer couldn’t nod its memory disks sympathetically, it repaid the women by instantly summarizing their difficulties and spewing out a ready-to-file lawsuit.

The women, low-income clients of the Cook County Legal Assistance Foundation, were part of a federally financed experiment to determine whether computers could handle the routine paperwork of divorce cases more efficiently and cheaper than lawyers.

If the divorce project was successful, officials planned to program the computer to become a vending machine for such other mundane legal documents as wills and bankruptcy petitions.

But after five years, the efficiency of divorce-by-computer is still in question. Lawyers for the Cook County foundation swear by it, but the authorities responsible for the project’s funds have reached a preliminary decision to abandon it.

“We had a 2½-year backlog of divorce cases until we got the computer in operation,” said Henry Browne, director of the project here.

“Finally, last year, we caught up. Without it, we would probably fall behind again. The secretaries (who were formerly responsible for preparing the paperwork) would hate having to go back.”

Original plans called for terminals resembling television sets to be placed in each of the three branch offices of the foundation to “ask” divorce clients 300 to 400 questions.

(The questions call for multiple-choice or very short answers, and the computer is programmed to base queries on previous answers. If a client says there are no children, for example, questions on the issue of custody are automatically dropped.)

Because so many of the clients have reading problems, or are unfamiliar with the English language, however, the foundation lawyers have found it better to use paralegal aides as intermediaries between the computer and the clients.

Though there are 11 grounds for divorce in Illinois, the computer is programmed only for the four most common; physical cruelty, desertion, mental cruelty and habitual drunkenness. Each interview lasts 20 to 40 minutes and, once finished, the computer rattles off more than a dozen documents required by the courts.

Since it was approved in 1971, the project has been stalled by hardware and development problems. Browne said breakdowns were so frequent and programming so slow that the first “live” interview wasn’t held until late in 1974.

Most of the 1,000 clients who’ve used the computer prefer it, Browne said, because they believe it will speed up their cases. The cost of the

project, however, is something he avoids discussing other than to estimate that each divorce handled by the computer costs about \$22 in machine time. "The total cost (of the project) isn't meaningful because it depends upon where you are. The actual figures are subject to misinterpretation. Most of the money has gone into development."

Harriet Ellis, a spokesman for the Legal Service Corp. in Washington (a private agency that receives funds from Congress to pay for the project), said: "The original purpose was to test whether the delivery of legal services in this way would be more effective. Last March, the corporation made a preliminary decision not to continue funding the project (after July 1) on the basis that divorce actions are not handled any more efficiently or cheaply by computer."

But that decision is being appealed by Browne, who contends that the denial was based on misinformation. "They (Legal Service Corp.) think the cost was one thing; we say it was actually much less. It's true the budget was \$120,000, but we never spent that much—sometimes we didn't even spend that much in two years."

[From the Computerworld, Mar. 1, 1976]

VOTE-CARD SWITCH PROMPTS SUIT CHALLENGING OUTCOME OF MAYORAL RACE IN MICHIGAN

(By Catherine Arnst)

FLINT, MICH.—An accidental switch of the computer cards in two voting devices influenced the outcome of the mayoral elections here last November, according to a recently filed lawsuit.

The "error" occurred in two precincts' Votomatic devices, which are small machines in which the voter punches a hole next to his candidate's name into a computer card inside the device.

In Michigan, the names of candidates are rotated on the ballot in every other precinct; a candidate's name would be on top of the list in one precinct and on the bottom in the next.

Two of the nine ballot books in the Votomatics in precincts 51 and 52 were switched so that a vote cast on those devices for one candidate would be tallied as a vote for the other candidate.

The cards themselves are not marked with the candidates' names. When they are tallied by the city's computer, all the cards in each precinct are tallied together.

There is no way the card can be traced back to the individual machine, and there were five Votomatics in one of the precincts and six in the other. Consequently, all 746 votes cast in the two precincts are in dispute.

The election was won by James Rutherford by a margin of 206 votes out of 42,000 cast.

The error was discovered only because a recount was ordered because of the closeness of the election. Even then the mistake was missed in Precinct 51; no error was realized until the votes in Precinct 52 were recounted.

"There was a foul-up when the booklet was inserted into the Votomatic prior to the election," City Clerk Gerald Brown said, even

though the election workers had been given extensive instructions to check the booklets.

Both the losing candidate, Floyd McCree, and the League of Women Voters have filed suit with Genessee Circuit Judge Ollie B. Bivens, Jr. requesting that the entire election be rerun.

It is believed there has never been an error of this type in Michigan or any other state before.

In other cases where election errors have occurred, there have been perhaps a 50/50 split on whether the election should be rerun, Barry Moon, attorney for the league, said. In New York State, "the general rule has been that, if there is more than a 3% chance that the outcome of an election would have been reversed because of the error, there is usually a new election," he said. In Hawaii, however, one chance in 100 would require a new election to be held, he said.

The Flint election is a test case in that it will decide the question of what a court's position should be in relation to the implications of a computer error on the outcome of an election, Moon said. "At what point does the court decide a new election should be held?" he asked.

"If the election is allowed to stand, whether the chances of there being a different outcome were one in 2 billion or one in 200, a precedent would be set so that, even if absolute fraud were shown, an election would be allowed to stand," Gordon Suber, attorney for McCree, said.

"There is so much apathy and distrust of elected officials now by the public, how could we tell the voter we can't even assure the accuracy of his vote when he goes to the polls? That would really be the bottom of the pit," he said.

The city's position in the case is that no new election is needed because the effect of the error on the outcome was so small.

EFFECT OF ERROR DISPUTED

Dr. Leo Katz, a mathematics professor, claimed in a document filed with the court that the mathematical possibilities of the switch having an effect on the elections outcome was one in a billion.

Richard Rosenberg, employed by the league as an expert, contended Katz used faulty data and assumptions when he assumed the voting devices in the two precincts were used by an equal number of people.

This was unlikely and contradicted by interviews with election workers, Rosenberg said. His findings were that the chances of the switch causing the victory to go to the wrong candidate would be one out of 11.

Rutherford said he feels that, as a general rule of law, it is not advisable to change an election over human error. If there is a new election, however it should only be held in precincts 51 and 52, he said.

CONSTITUTIONALLY UNSOUND

"The big issue now is whether there should be an election in just those two precincts or the entire election should be rerun," Moon said. It would be constitutionally unsound to hold an election in just the two precincts in contention, he stated.

The league's position is that to allow only those two precincts to revote would put "a premium on fraud," Moon said.

About 98% of the people would be letting 2% of the people decide an election for them, if only those two precincts revoted, Suber said.

In the future, there will be three additional checks in the procedures after the booklets are inserted in the Votomatics and before the polls open, Brown said.

"When you're dealing with humans there are bound to be errors. Some of these election workers work only three days out of the year. We'll just have to emphasize the checks more in the future," he said.

POSSIBILITY OF FRAUD

Although both McCree and the league agree that this error was accidental, they also claimed the same switch could easily be done on purpose with Michigan's system.

"I'm satisfied that, for a very small amount of money, anyone could manipulate the outcome of an election by getting at just one computer operator," Suber said. "I'd rather go back to hand ballots, where there is less possibility of fraud," he added.

It would be fairly simple to determine which precincts would vote most heavily for a certain candidate and then change the cards in that precinct, Suber and Moon said.

"Those two particular precincts were predictable as to who would be voted for; if there was going to be fraud, those precincts would be ideal," Moon said.

It had been predicted McCree would win over 80% in one of the precincts where the error was made and, "it would not be surprising if he had won over 90%," Suber said.

In the actual election, however, he got less than 60% of the vote in that precinct.

The impact of this error is very severe, Suber said. "And what is the difference between fraud and error?" he asked. "The only difference is the intent of the party. I could be a complete idiot and commit an error just as serious as if I were trying to do it on purpose. The issue of human error will still exist despite any additional checks," he said.

An official with the Michigan State Election Committee said no plans are currently in the works for changing the voting procedures in the state and would not comment on the possibility of fraud with the present system.

Approximately one-third of the state now uses voting devices similar to Votomatic, which was authorized for use 10 year ago. "It's probably the coming thing" for the rest of the state, the official said.

[From the Computerworld, Mar. 8, 1976]

MANAGEMENT SEEN DOING TOO LITTLE TO CURB DP CRIME

(By Molly Upton)

SAN FRANCISCO—Corporate managers could be doing more to prevent losses perpetrated with the aid of a computer, according to panelists at a session on "How Are Computers Being Used to Aid the Criminal?" at the IEEE Computer Society's Comcon 76 spring meeting here recently.

There is relatively little need to penetrate a system in a sophisticated manner since there are so many easier accesses, Donn B. Parker of Stanford Research Institute and Brandt R. Allen of the University of Virginia agreed.

Parker recommended tightening up the obvious areas, such as physical access, and protecting I/O from disclosure and modifications.

It is up to management to slow down developments in the computer area until the gap closes between auditing ability and applications that may be on the leading edge of technology, Allen said.

Too often management has abrogated its responsibility for the protection of the firm's assets, he said. Management has a right to—and should—slow down advances until it knows all procedures involving the firm's funds are secure, he said.

IMPROVING ENVIRONMENT

Another area in which management should be doing more is making corporate DP areas a better place to work, Allen said. Business DP firms are generally not pleasant places to work in, he added.

Calling computer people somewhat of a "problem" because they're "different, difficult to manage," he said organizations are not dealing with problems of burnout and technological change.

Allen suggested the current method of making an auditor knowledgeable in DP is the backward way to solve the gap between state-of-the-art DP auditing and the tasks to be done.

Since he believes computer people are born and accountants made, it would be easier and more effective to turn some DPs into auditors, he said.

Management should install control points between programming operations and data preparation and other phases, he said. The responsibility should be separated to ensure that a program, once written, is not updated without the proper procedures.

Firms have the ability to tighten physical security, but many are not doing it, he said.

Verification of on-line users is a problem from a technological view, but from an administrative view it is even worse, Allen said.

Operating systems are not a major problem for most businesses since the other areas are easier to penetrate, he added.

WHITE-COLLAR CRIME

Parker said he emphasized tightening the obvious security points because white-collar crime occurs where the people are. "White-collar crime varies inversely to automation," he said.

In the future, there could be a reduction in white-collar crime simply because there will be fewer people in these areas as automation takes over.

The average loss per case will rise astronomically, Parker predicted. In 1975 the average loss in bank cases, according to Federal Bureau of Investigation reports, was \$19,000, whereas the loss involving DP was \$450,000, he said.

Of 362 computer abuse cases, 147 occurred because of poor controls on manual input and output, he said. Weak or absent physical access

controls were found in 46 cases; weakness in computer and terminal operations, 43 cases; and failure of business ethics was the cause in 41 instances.

Poor control of programs was responsible in 33 cases and lack of operating system access controls and integrity occurred in 24 instances.

In 120 cases, the scene of the action was in the data and report preparation facilities, Parker said.

"NO EMBEZZLEMENT REVOLUTION"

Allen said "there is no revolution in embezzlement" despite the use of computers.

In the majority of cases, the deed is done through altered transactions, he said. The type of embezzlements are the same as years ago, involving disbursements, billing, payroll, inventory and receivables, he noted.

Allen estimated computer fraud could be approaching \$100 million a year; much goes unreported by corporations, so it is difficult to estimate, he added.

Edmond L. Burke of Mitre Corp. said one method of devising a secure system is to implement a reference monitor at the kernel of a system.

This monitor would have an audit mechanism to provide accountability for each access by monitoring log-ins, length of sessions and CPU time used. It would be isolated so it could not be tampered with and should be designed and built so its correct operation can be verified, he said.

Mitre is building a security kernel for the Multics system and an operating prototype should be available in about five years, he said.

But then it will be up to the "fickleness of the marketplace" to determine whether such an item is in demand, he observed.

[From the Computerworld, Apr. 26, 1976]

REDTAPE TYING UP PROGRAMING OF FEDERAL IMPACT AID FUNDING

(By Esther Surden)

WASHINGTON, D.C.—Complex federal legislation is causing problems in computerizing Impact Aid payments for this fiscal year, according to the Department of Health, Education and Welfare (HEW) spokesmen.

However, the Impact Aid checks are being issued without delay, despite difficulties translating new funding provisions of the law into computer programs, according to Thomas J. Pritchard, acting chief of the Technical Assistance Section for the Office of Education.

Impact Aid is a program that allocates federal money to school districts with children whose parents live or work on federal property, HEW said.

"For about 18 months" the HEW computer center personnel had been "trying to get policy set, procedures established and methods of making payments defined," Pritchard said.

"We in the computer department do not make those policy changes; we do not change programs until the policy is known. The system hadn't even started to be changed until January of this year."

The original Impact Aid legislation was enacted in 1950, but recent amendments to the laws called for the restructuring of the allocation methods, HEW said.

"The legislation changed categories, changed provisions of how payments would be made," Pritchard continued. "What they (the programmers) are doing is making payment formulas, and you can't make the formulas until the people decide what percentage will be paid for what reasons," he added.

Rather than continue with the old method of funding or take a chance that the new system wouldn't be up on time, HEW sent payments amounting to 50% of last year's funding to each of the schools, Pritchard said.

When the completed computer program is run on May 1, the deadline for the programming effort, "we'll just recompute" and distribute the funds owed, Pritchard said.

The Division of School Assistance in Federally Assisted Areas (SAFAA) normally makes partial payments throughout the year, so the 50% partial payment doesn't represent a hardship for the schools involved, he said.

The Impact Aid program was extended to 1978 through the Education Amendments of 1974, which also called for the restructuring of the funding provisions as of fiscal 1976, HEW said.

The Education Amendments legislation is implemented via regulations, an HEW spokeswoman said, and the regulations in question were not developed until Dec. 5, when they were published in the *Federal Register*.

The programs are being run on an IBM 370/168 and a 370/165; five people are involved in the programming, Pritchard said.

[From the Computerworld, May 3, 1976]

MASSACHUSETTS WELFARE DEPARTMENT HIRES DPERS TO PINPOINT CHEATERS BY MATCHING LISTS

(By Nancy French)

BOSTON.—The Massachusetts Department of Public Welfare has hired a specialized DP service group here to help match 6 million personal records this year in an effort to spot welfare cheaters.

The program is expected to reduce overpayments and eliminate payments to ineligible recipients—errors that now cost the state an estimated \$7 million to \$10 million a year, according to Commissioner Alexander Sharp who heads the welfare department.

Besides assuring no recipients are illegally receiving more than one type of public assistance, the program is expected to provide fraud safeguards and ultimately increase child support revenues, according to Sharp.

Urban Data Processing, Inc. (UDP) of Burlington, Mass., won the competition for a one-year \$184,000 contract that involves combining lists of recipients of Aid to Families with Dependent Children,

General Relief, Food Stamp and Medicaid with information contained in the files of other state agencies.

But combining a couple of mailing lists with different structures and formats for name and address files is no easy task.

UDP will do the job by first "normalizing or standardizing the formats as well as the components within each field on every agency's list of recipients, Max Eveleth Jr., UDP president, explained.

Using proprietary software systems known as the Street Address Matching System (Sams) and the Customer Information System (CIS), UDP will disaggregate each original record furnished by the state. UDP's software is based on pattern recognition and table lookup techniques, he said.

RECORD CREATION

New records, organized by name, street address, city, state, Zip Code and file source code will be created. The records will also contain other variable data that in some cases includes Social Security number; however, the Social Security number will not be used as a key in matching, he emphasized.

UDP's programs were originally developed for use by banks that wanted to get a thorough picture of their customer's accounts and dealings with the institution, to see what other services each customer could be encouraged to utilize, he explained.

The state will furnish the lists on magnetic tape; processing will be done at UDP; and the names, matched in accordance with welfare department's predetermined criteria, will be returned to state personnel, ready for printing, according to Harry Kreide, project manager in the welfare department's DP center.

Specialists will determine whether certain records are simply duplicate, whether the address data is incorrect or out of date, or whether in fact the recipient appears to be cheating, Kreide said.

If evidence of cheating is found, caseworkers will follow up with an investigation of the case involved.

PRIVACY ASSURANCES

To assure the privacy of recipients, no printing will be done by the contractor, Kreide said.

In addition, UDP will be bound by all the privacy regulations and standards that govern the welfare department itself, and these will be specified in the contract, he added.

In addition to matching the files, UDP will help the Department of Public Welfare convert the software so that, by the end of the one-year contract, the programs can be run on the department's internal system.

The software was written for use on an IBM 370/158, running under OS/VS, whereas the state uses an IBM 370/145 running under DOS.

Fifty percent of the cost will be reimbursed by the Federal government, according to Sharp.

The new matching system is expected to be a great improvement over methods used previously which were limited primarily to cross-checking Social Security numbers, Kreide indicated.

[From the Computerworld, May 10, 1976]

PRIVACY PROTECTION SEEN BACKFIRING ON INDIVIDUALS

(By Catherine Arnst)

CHICAGO.—Should the most important concern of privacy legislation by the individual's right or the public good? This question was posed by two speakers at the Human Services Information Systems Conference held here last week.

Although the Privacy Act of 1974 was meant to protect civil rights, that protection can backfire on Welfare recipients, the speakers said.

Applying the provisions of the Privacy Act to public welfare can be a "double-edged sword," James Trainor, director of state systems management at the Department of Health, Education and Welfare (HEW) quoted a former HEW Secretary as saying.

The present HEW Secretary, David Mathews, once said: "there are good sound reasons for collecting many types of information. Without adequate records, older Americans would not receive their Social Security checks.

"But the potential for careless or mischievous use of private information is a fact of private information is a fact of modern life that we ignore at peril to our liberties as a free people."

The public welfare system "depends on an exchange of data between agencies to do a good job. When we deal with clients requesting services, we ask them to lay their souls bare," Charles McDermott, comptroller of the Oklahoma Department of Institutions, Social and Rehabilitation Services, said.

The situation has improved, however, McDermott said. An example of a less subtle time was 14 years ago, when Congress employed "night riders" to obtain information on welfare households in Washington, D.C., by visiting them in the middle of the night, he said.

Welfare agencies must obtain an extensive amount of personal data on their client and then store all this information, McDermott said. "There's enough data stored on an individual to ruin his life forever. But, that's not much different from what any large corporation does," he said.

The Privacy Act has forced state agencies exchanging information to develop methods of complying with both the act's regulations and those of HEW, McDermott said.

The Parent Locator Service, which states are required to have to qualify for certain federal funds, is one area where privacy requirements and HEW requirements have to be made compatible.

With the Parent Locator Service, exchange of information is permitted without the consent of the individual, but the Privacy Act prohibits exchanging the Social Security number (SSN). Without the SSN, it is very difficult to obtain the necessary data required by the service.

Some federal regulations have allowed agencies to get around this "Catch-22" by applying another: Individuals requesting benefits do not have to provide their SS numbers, but they can be refused those benefits if they don't.

The Social Security Administration (SSA) has gone to what may seem like extreme lengths in refusing to release the SS number, even

when that release could benefit the individual. McDermott said, "SSA is not trying to be unreasonable; it only wants to avoid breaking the law," he said.

The Privacy Act affects data exchanged between agencies in different states and federal agencies, but the proposed H.R. 1984 would extend these regulations to both agencies within a state and private agencies.

In looking toward a future that could include H.R. 1984, McDermott suggested that public and private agencies develop an awareness of impending legislation in order to avoid problems.

Whether or not both the Privacy Act and H.R. 1984, if passed, will ultimately harm more than protect Welfare recipients is a determination that neither he nor HEW as a whole could make, Trainor said.

CLIMATE CHANGED

"We're not monolithic at HEW; we don't have a corporate line," he said. The climate of the government has changed radically in the last few years, he added.

Under Nixon, the privacy of Welfare recipients was meaningless because the attitude was "that the bums should be off the rolls anyway," he said. After Watergate, the government and HEW switched to the other extreme and demanded protection of privacy above all else. "Now, we're changing again," Trainor said. The attitude of the new secretary of HEW is that "we must have accountability, but we must also guard against abuse," he said.

"There's nothing wrong with asking someone applying for aid what his income is," Trainor said. What is wrong to ask and whether accountability or privacy should be the first priority are questions Trainor could not answer. He doubted that anyone at HEW could answer them.

[From the Computerworld, May 9, 1976]

UK JOB-MATCHING PLAN ATTACKED ON PRIVACY GROUNDS

(By Joe Hanlon)

LONDON—A computerized job-matching scheme which would rate job seekers according to their "suitability" for employment has drawn considerable protest here.

The pilot project, slated to begin this summer, "is in danger of running contrary to the principles laid down in the white paper on 'Computers and Privacy' [CW, Dec. 31-Jan. 5]," according to Gerry Fisher, deputy president of the British Computer Society.

And the Civil and Public Services Association has said its members, who work in employment offices, will refuse to do the ratings.

Under the proposed system, job seekers would be rated A, B, C or D. While employment officers have always done informal ratings, this is the first time the ratings would be formalized and passed on to other people.

The pilot project will use a Honeywell 66/20 to do on-line real-time job matching at 14 East London employment offices which annually place almost 30,000 people in jobs.

If successful, the matching project will be expanded to all of London.

INITIALLY SIMILAR

For the job seeker, the procedure will initially seem little different than it is now. As at present, the employment officer will take down details about the applicant.

Instead of searching through a file box of slips of paper for jobs, however, the officer will input the data via CRT and immediately get a list of any appropriate jobs. The job seeker can then go for interviews.

The radical change in procedure will come when there are no appropriate jobs immediately available. At present, if an employer telephones an employment office with a job, the opening is circulated to employment officers, who decide which of their clients to send for an interview.

With the new system, the computer will print out a list of all appropriate people, listed in order first by nearness to the job and then by "suitability". The decision on who to send for interviews will be made by an officer at the employment office nearest the job.

The officer will be making choices about people he has never met, based only on data from the computer. And the officer can pass over nearby people with low suitability ratings to choose people farther away with higher suitability ratings.

The suitability rating will be based on job stability, employment record and "realism." But the Employment Services Agency, which will run the system, refused to say if a person could see and challenge the rating, although the white paper said this should always be done.

Suitability will be listed on the CRT screen as "JOB CAT." so it is not clear how many people will even know what it is.

Data from employment offices is available to social security and welfare officers under many circumstances, and observers believe it likely that "suitability" ratings will find their way into many welfare files. Employers will probably be permitted to ask for certain suitability ratings, and thus they too will find out this information.

The Manpower Services Commission, which runs the Employment Services Agency, announced last month it had approved the use of suitability ratings. The commission attached particular importance to the review procedure, which would obviate any possibility of the so-called "tag-for-life."

This review procedure will require that people who do not get jobs within a fixed period be interviewed by a different employment officer who can revise the computer entry.

But the British Computer Society is still unhappy. The scheme "might eventually invalidate the claims made in the white paper as to the strict controls exercised in the public sector on personal data. Coming as it does at the height of the privacy debate, it could possibly seem a rather rash proposal," Fisher commented.

According to Fisher, one of the biggest objections is that the Manpower Services Commission made the decision in secret—despite the white paper's argument that such choices should be made publicly.

The Manpower Services Commission "knew the white paper had been published, yet it chose to make its decision privately, leaving it to be dug out by journalists. Even if it is a perfectly good scheme, by

failing to discuss it publicly it is asking for every bit of trouble it is going to get," Fisher said.

[From the Computerworld, May 17, 1976]

STUDY SEES COMPUTERIZED NATIONS MORE VULNERABLE TO WAR THREATS

(By Catherine Arnst)

STOCKHOLM, SWEDEN.—The wars of the latter half of the 20th Century have tended to break out in underdeveloped, "third-world" nations where automation is still a stranger.

But those nations advanced enough to be submerged in computerization could be even more vulnerable to the threat of war, a study recently released by the Swedish Ministry of Defense contended.

"Computerization presents new and efficient methods for creating chaos and confusion in the community with very little effort," according to the study of Sweden's dependence on computers, titled "The Vulnerable Computer Society."

The Secretariat for National Security and Long-Range Defense Planning, which prepared the study, said the result of increased dependence on DP will be that "many of the peacetime functions in total defense will be so dependent on computers that it will take vast emergency planning and expenditure to ensure defense can fall back on manual routines in the event of war."

It also warned that the interaction between and interdependence of computer systems could mean that "a completely trivial event, such as the failure of one data system, may have far-reaching consequences for large sections of the community."

Although such events can occur in peacetime and still cause considerable problems, "it seems even more reasonable to assume that such events are more likely to take place during periods of what can be loosely termed 'social stress,'" the report said.

"IRREVERSIBLE PROCESS"

The problem with automating a large number of processes in a society is that "the introduction of computers would seem to be an irreversible process, i.e., it is impossible to return to former production techniques . . . once processes have been computerized."

"Of course, this considerably increases the sensitivity and vulnerability of society to different kinds of upsets," the report said.

The computerization of certain functions would particularly lead to a pronounced heightening of vulnerability, the report said.

These functions include activities previously dominated by labor-intensive techniques requiring the handling of large quantities of data, such as bookkeeping, advanced surveillance and control of complicated courses of events, such as traffic surveillance and control.

The computerized control of production processes in the manufacturing industry and real-time processing, which has made it possible for several users to be in direct contact with the computer via remote terminals, were also cited by the report.

IDEAL TARGETS

Data banks which contain detailed information on a country's population are ideal targets for "a possible aggressor who is trying to gain effective and complete control of the population when engaged in acts of war," the study warned.

Data communications between nations are also extremely vulnerable; facilities for an effective control of the information moving between countries are very limited, it continued.

"International movements of data should be kept under very vigilant surveillance," it urged.

The greatest danger to a computerized society in time of war is its computers, the report emphasized. Not only is it difficult to operate a society dependent on computerization during war, but "it is possible for an aggressor to choose targets so that by spot strikes on DP systems he can achieve both great psychological effects on the entire population and the total disruption of local production and community services.

"Expanding computerization will probably require new and much more comprehensive security measures in order to safeguard the administration of society in the broadest sense of the term," the study recommended.

[From the Computerworld, May 17, 1976]

JAIL SUICIDE BLAMED ON TERMINAL OPERATOR

(By Nancy French)

YONKERS, N.Y.—The jail suicide of a 20-year-old man here has been blamed largely on a police communications employee who "misinterpreted" a standard National Crime Information Center (NCIC) computer code.

But three other factors also contributed to the youth's death—insufficient training of police communications employees, an improperly canceled warrant and NCIC's practice of retaining cleared warrants in its data base, according to Eugene Fox, counsel for the city of Yonkers, and Lt. John Duffy, the police officer who investigated the conduct of the policemen involved.

Steven Karagianis was found dead in his cell one and one-half hours after he was arrested by a Yonkers police officers on a warrant for probation violation that had been canceled a month earlier [CW, April 26].

The civilian communications employee on duty in the police station when the youth was arrested was a former Marine Corps teletypewriter operator with only 16 hours of training in communications at the Yonkers Police Department, Duffy said.

The operator read an NCIC record coded "CW" as "Current Wanted" (no such code actually exists) rather than "Cleared Wanted." Instead of checking with superiors who could have helped him, he radioed incorrect information to a police cruiser, the investigation found.

Duffy, who heads the Yonkers Police Department's Internal Affairs Division, explained the sequence of events on the night of the suicide as follows:

At 11:24 p.m., Karagianis was stopped for going through a red light. In accordance with routine procedures, the police officer who stopped him radioed the communications operator for a record check on the automobile and driver.

Using the New York State Police information network, the communications operator requested an "R and All," or "record and all other information," Duffy said. New York State's criminal justice computer had no record on Karagianis, nor did the Department of Motor Vehicles, he added.

The response from NCIC showed an active warrant, however; it was coded "CW," meaning the wanted individual had been apprehended, action had been taken and he was no longer wanted.

OPERATOR WRONG TWICE

The communications operator misinterpreted the message and radioed inaccurate information to the cruiser; the patrolmen brought Karagianis in.

Since the youth protested so strenuously that the warrant had been canceled, the operator was instructed to resubmit the inquiry, but the same messages came back.

"He misinterpreted the NCIC message the second time the same way he did the first time," Duffy said.

The improper cancellation of a warrant was also cited in the investigation report.

Karagianis, who had been serving five years' probation for a minor marijuana offense, was picked up a second time last November and charged with violating probation.

He appeared in Westchester County Court in January, at which time the charge was dismissed, and the warrant should have been canceled—not just cleared and left in the NCIC data bank, according to Duffy.

Karagianis' attorney, Jeremiah Gutman, became aware the warrant had not been canceled when police came looking for the youth on March 4. On March 5, the attorney wrote a letter to the Sheriff's Department; records indicate the warrant was cleared but not canceled on March 9.

Rather than sending the clear order to the attention of the Yonkers Police Department, however, the notice was sent as an "all points bulletin," which was overlooked in the yards of generalized teletype-written messages the Yonkers Police Department receives each day, Duffy found.

When Karagianis was arrested, the police actually had both the warrant and the notice, but the two had not been matched up, according to Fox.

New training classes have begun at the Yonkers Police Department to review all NCIC codes and procedures, according to Duffy, and disciplinary action is expected to be taken against the communications operator.

[From the Computerworld, Jan. 6, 1971]

RADAR WIPES OUT IRS TAPES; CONSULTANT CITES POOR GROUND

(By Edward J. Bride)

NASHVILLE, Tenn.— Several, perhaps hundreds of Internal Revenue computer tapes containing thousands of tax records were erased by airport radar last spring, and some of the data has not been restored yet.

The then brand-new computer center here is “within a couple hundred yards” of a radar installation, according to a tax official, and a consultant has revealed that inadequate grounding of metal shielding was the cause of the wipeout.

Information is still sketchy at best, since IRS officials contacted by CW would not discuss the matter, other than denying knowledge of its occurrence and promising to “look into it.”

But the consultant who assisted the tax agency in revealing the problem said the IRS reticence was due to the fact that there were no duplicate files on some of the 1969 returns involved.

The consultant, Henry Hoffart, also stated “hard copy” original returns and documentation from the previous years had been put onto computer tapes for comparisons, and that this information, too, was lost.

Hoffart is director of electromagnetic compatibility research for Topaz Electronics, of San Diego, but was a consulting engineer for General Electric when the tax record wipeout occurred.

SPURIOUS ENERGY

He said that if the center had had effective grounding, the “spurious energy” from the airport radar would not have affected the computer tapes.

Another consultant told CW that computer centers in “high ambient areas” those near radio transmitters, for example, could experience similar difficulties, especially without adequately grounded shielding.

Hoffart criticized grounding regulations of the Army Corps of Engineers, which permit aluminum conductors for grounding. Low-conductivity aluminum allows more “noise” on a circuit, he claimed.

The Army Engineers also require only one ground for computer center, according to Hoffart, and this ground is at the entrance of the power to the building.

Hoffart noted that at the Austin, Texas, IRS center, the computer is removed by about 500 feet of cable from the ground, the processor is “sitting up in the air,” making the computer a transmitter at certain wave lengths.

He said such a construction could make the computer a receiver, too.

He said inadequate shielding, or ineffective grounding of proper shielding, can compromise the security of data being processed, and receiving equipment could eavesdrop on police information or other sensitive messages.

[From the Washington Post, June 16, 1976]

THEFT BY COMPUTER—CONVICTION CALLED LANDMARK

(By Donald P. Baker)

A Lanham man whose burglar tools were a computer terminal, a telephone and an extremely clever mind was convicted in U.S. court in Baltimore this week of tapping into a computer that contained classified files of the Federal Energy Administration.

Punching secret passwords into a keyboard computer attached to a telephone in his Alexandria office, the defendant, Bertram E. Seidlitz, dialed the telephone number of the computer firm in Rockville where the FEA information was stored and extracted 40 rolls of computer printouts before he was caught.

U.S. Attorney Jervis Finney said the tapped computer contained classified data relating to oil and other energy resources of the nation. The federal prosecutor said the computer-age theft "signals the future of white-collar crime."

Stan Neeley, president of Optimum Services Inc. (OSI), the Rockville firm that has a \$7.3 million annual contract to provide computer services to the FEA, said the information Seidlitz obtained was valuable not because it divulged FEA secrets but because it would permit computer firms to duplicate the complex system used to store the FEA data.

Neeley said the conviction was a "landmark" in the computer industry, "which needs to find a method to protect its assets from theft."

Seidlitz, 38, of 8629 Brae Brooke Dr., Lanham, admitted the theft but he said he did it only to show how lax security was at OSI, where he formerly was employed.

Neeley said OSI, which has 1,300 employees throughout the country, is a large federal contractor that also performs computer work for the Federal Trade Commission, Environmental Protection Agency and the Departments of State and Labor.

Neeley said the only reason Seidlitz was able to tap into the computer was because he was a former employee "who retained in his memory the keys to unlocking the information."

The computer fraud was discovered by an OSI employee who was monitoring the computer and "detected an unauthorized user on the line accessing the computer," Neeley testified at the trial, which ended Monday.

The trial, before U.S. District Court Judge Alexander Harvey II, lasted eight days. Because much of the testimony was offered in computer jargon, much time was spent translating the technical terms into words the jurors could understand.

Defense attorney Frank M. Kratovil of Hyattsville argued that Seidlitz wanted to show "in good faith" to the FEA that OSI's computer "could be accessed."

From Oct. 19, 1975, through Jan. 9, 1976, Seidlitz secretly withdrew from the OSI computer 18 of the 20 codes needed to extract information from the Wylbur program and its companion program, Milton, which are used by OSI to store the FEA data. (The programs were developed at Stanford University in the mid-1960s, and were named

for the Wright brothers and their father, according to Neeley. The third program, Orville, was not involved in the theft.)

OSI, whose national headquarters is in Santa Clara, Calif., bought Wylbur, Orville and Milton computer systems from Stanford, and Neeley testified the company spent \$100,000 improving them.

The sophisticated systems give OSI a competitive edge that has resulted in \$30 million to 40 million in contracts, Neeley said.

Roger Fajman, one of the original designers of Wylbur at Stanford and who now is a computer specialist at the National Institute of Health, testified for the defense. His testimony indicated that it would have been difficult for Seidlitz to convert the Wylbur program for use with the computer that Seidlitz' company rents.

The system is valuable because of its ability to handle more users than some competitive systems, and because it responds to simple commands that makes it easier for novices to operate, Fajman explained.

When the OSI employee detected the unauthorized user of the line last Dec. 30, company officials contacted the C & P Telephone Co., which traced the call to Seidlitz' computer firm in Alexandria.

The next day, the unauthorized user was back at work, tapping the computer, but that time, OSI got a duplicate printout, which it gave to the FBI.

Using a court ordered search warrant, the FBI raided Seidlitz' office at 300 N. Washington St., Alexandria, on Jan. 9, and recovered the computer printouts.

A second search warrant subsequently recovered the portable computer terminal and a diary that showed entries relating to the plan to steal the Wylbur program, Finney said.

Seidlitz, a mid-level executive who worked at OSI from Jan. 1 to June 17, 1975, was described at the trial by computer expert Robert Fitzgerald as "an extremely clever systems programmer" who is a highly qualified technician and mathematician.

Neeley said Seidlitz "technically resigned by mutual agreement" last summer. Before he left, according to Seidlitz' testimony, he frequently had complained about the lack of security on various U.S. projects there.

Finney, who was aided in the prosecution by Assistant U.S. Attorney Robert A. Rohrbaugh, said conviction of fraud by wire could result in fines of \$1,000 and imprisonment for five years on each of two counts. Seidlitz will be sentenced after completion of a presentence investigation.

UNIVERSITY OF FLORIDA



3 1262 09113 1721