CONSIDERATIONS FOR SECURITY IN ELECTRONIC
DATA PROCESSING

Lynette Sprague

Honors Project
Dr. Elias M. Awad
April 9, 1976
OUTLINE

I. Physical Security of the Installation
   A. Prevention of accidental destruction
      1. Choosing a site
      2. Considerations in case of natural disaster
         a. fire
         b. flood
         c. power failure
         d. recovery from the above
            1. back-up
            2. insurance
   B. Prevention of intentional destruction or disclosure
      1. Theft
      2. Sabotage
      3. Eavesdropping

II. Data Security and Control
   A. Prevention of accidental destruction, modification or disclosure
      1. Programmer error
      2. Operator error
   B. Prevention of intentional destruction, modification or disclosure (access control)
      1. Unauthorized access
         a. considerations for on-line real-time systems
         b. file control
c. cryptography
d. control of documentation

2. Authorized access (personnel)
   a. operator fraud
   b. programmer fraud
   c. embezzlement
   d. auditing

III. Need for Security

IV. Cost of Security
CONSIDERATIONS FOR SECURITY IN ELECTRONIC
DATA PROCESSING

Today the computer plays a mandatory, vital role in society. Computers are used to dispatch police and ambulances in emergencies, to prevent collisions through an air traffic control system in large airports, to store trade secrets for oil companies worth millions of dollars to competitors and to control the targeting and launching of both U.S. and Soviet intercontinental ballistic missiles. Obviously, there is more than just money at stake in the multimillion-dollar race for computer security. The possibilities for major theft or destructive sabotage via computer are staggering. It is estimated that computer-theft losses in the United States run billions each year and that for every computer crime that is uncovered, ten are thought to go undetected.¹ One assurance must be certain: that vital data is not lost in the data processing function, that errors are not intentionally put into the system and that unauthorized persons do not have access to the system to read or modify data. One must be aware of the need for security of the data processing center, the precautions and actions which will assure this security and the cost of implementing and maintaining sufficient security procedures. Security of the data processing function can be divided into two considerations: The need for physical security of the computer installation

and the need for data security within that installation.

Physical security includes considerations in the prevention of accidental or intentional destruction of computer equipment, files, and documentation. The environmental factors surrounding a data processing function determine its vulnerability. For this reason the physical planning and structure of an installation is of utmost importance. A balance must exist between security and operational efficiency. The first consideration when a new building is intended is its site. Because a computer installation merits special protection which a normal office building does not usually need, it should ideally be a separate structure. The advantages of a separate building for the computer installation are these: fire protection and access control are made easier because resources can be concentrated where they are needed; the likelihood of office personnel and computer staff secretly showing data for the purpose of fraud, etc. is reduced and the opportunity for computer staff to have access to other offices when they are working after normal hours is eliminated. Before a site is chosen the area should be investigated to determine the likelihood of flooding (namely rivers and canals), explosion from near-by buildings (storage of large quantities of combustible materials such as paint or gasoline), and interference with the computer's electrical signals (radio or radar equipment near-by). The facility should also be located away from airline flight paths, railroad tracks and highways.\(^2\)

Necessary precautions must be taken in the prevention of accidental destruction of the computer installation from such things as fire and flood. One of the most obvious and overlooked protective measures is simple observance of fire protection rules. Installation of such protective measures as sprinkle-systems and fire extinguishers should be made but they must be placed in effective locations. Robert Courtney, manager of data security and privacy at IBM, recently said at the Data Processing Management Association conference in Atlanta, Georgia, that there is a tendency to place "all fire-quenching equipment where the most dollars are, rather than where the most flammable material is located." He gave the example of a company which spent $180,000 installing fire-extinguishing equipment in its computer room, but had no fire-prevention equipment in the cafeteria's kitchen, which was directly underneath. "All it did was spend $180,000 exercising its option to bake instead of fry," he said.3

In the case of electrical power failure, back-up power must be provided for the computer equipment and air-conditioning. The great Northeastern power blackout in November 1965, clearly illustrates that no segment of our country is immune to electrical power failure. A few milliseconds of 10% power fluctuation can cause not only a temporary interception of computer processing, but inherent damage to the electronic circuitry which could cause equipment failure.

3Catherine Arnst, "Incompetency Seen as Major Threat to Data Security," Computerworld, July 16, 1975, p. 5.

Back-up should be maintained for all vital files, programs and documentation in another location to be used in the event of natural disaster. There should be well-established procedures which are practiced for protecting files, programs and hardware against fire hazards. Personnel should be prepared to use back-up equipment in emergency and even be able to temporarily process critical data manually.

Most companies are aware of the potential risks involved with fire, flood and natural disaster but other potential hazards are frequently overlooked. "Lack of a complete set of back-up files caused a serious problem for one company. An employee, who was cleaning the interior of a magnetic drum cabinet, attached his magnetic flashlight to the frame of the unit. The magnet destroyed a portion of the data on the drum, a portion which the company did not ordinarily duplicate. The company lost six days of computer time reconstructing the lost data."5 In addition to the need for back-up files and programs, this example illustrates the necessity to train the personnel who maintain computer equipment adequately. Recovery and back-up checklists may be found in Appendix L.

Security is meaningless without adequate insurance coverage. Increasing investments in computer hardware (if owned), program development, and stored data make it vital for management to constantly evaluate a company's coverage. Management should

question themselves as to whether or not their present coverage would sufficiently cover substantial financial loss in the event of an EDP system disaster from fire, flood, natural disaster or theft.

Intentional destruction or theft of equipment in a computer installation is just as important a security consideration as is potential loss from natural disaster. Theft, sabotage and eavesdropping are important security considerations. Unrest on college campuses recently have made EDP managers more aware of this problem. In Montreal, Canada, at Sir George Williams University, students had set fire to the computer center, causing an estimated $1 million damage to computer equipment not even considering the damage done due to the loss of the data processing function. Militant students at Brandeis and Northwestern Universities held the computer "hostage" to make their grievances known.⁶

Theft is a major concern in data processing today. Payroll information, accounts receivable and payable and inventory records could cost a company millions of dollars if they were stolen. It is known that people have been paid by a competitor to steal a company's tapes and disk packs containing trade secrets and vital data. Entire computers have even been stolen in the past by students, employees or whoever. In early 1969, a $2,500 Wang Computer disappeared from the Argonne National Laboratories. Later it was traced to Iowa State University by the FBI. A student in a

⁶Tbid.
training program at Argonne had liked working with the computer so well that he took it back to college to do his homework. Unless greater security precautions are taken we can expect to have more of stolen computers as they decrease in size. Data Processing Security, Inc., of Arlington, Texas had developed a device which will detect a tape or disk which is being removed from a data processing center. When detection occurs, an alarm alerts the security officer or individual on duty that a tape or disk is being removed from the premises and appropriate action can be taken. The system is supposedly not fooled when tapes or disks are placed in a box, briefcase, handbag, under a coat or on the body.

This computer has occasionally been a target for disgruntled employees, antiestablishment rebels, antiwar protestors and unhappy students. This has resulted in a number of serious sabotage attacks on computer centers. It was reported in The Wall Street Journal that an employee quickly stopped an important purchasing program because he erased the entire data records. To some persons the computer represents the fear of unemployment or mindless authoritarianism. Data processing managers developed real concerns about sabotage in the 1970's when it became highly publicized. Protestors from the Students for a Democratic Society succeeded in erasing 1000 tapes from Dow Chemical.


9 Ibid.

Today, a single reel of magnetic tape in a data processing center may contain well over 100,000 records. These records can be destroyed in seconds by placing an easily purchased magnet next to the reel of magnetic tape. A device has been developed which will detect a magnet when it is brought into the area and an alarm sounds to alert a guard.\textsuperscript{11} The approach to preventing sabotage should be: (1) minimize the likelihood of them wanting to do it (2) make it as difficult as possible and especially make the dangerous methods difficult.\textsuperscript{12}

Eavesdropping can occur in the form of wiretapping, snooping through wastepaper bins for carbon copies of listings of sensitive data, etc., visual eavesdropping such as learning a security code by watching a display screen or printout over somebody's shoulder, taking pictures with cameras or using bugging devices. A source of military intelligence for decades has been the recording of electromagnetic radiation from electronic devices. Some terminals emit radiation which can be picked up at a distance of 1/2 mile. Although this method is mostly used in the military, if security measures are tightened up to prevent access of data by other means, electronic eavesdropping may become a commercial problem. As of now it is nearly impossible to detect or prevent electronic eavesdropping.\textsuperscript{13}

\textsuperscript{11}Scoma, p. 21.
\textsuperscript{12}Martin, p. 324.
\textsuperscript{13}Ibid., pp. 342-345.
In a world in which the data processing function is so vital, it is of utmost importance that all possible preventive measures and precautions are taken to protect the installation from physical destruction which can occur accidentally or intentionally. A series of checklists can be found in the appendices which may provide direction in providing for the physical security of the data processing center.

A data processing function can only be effective and useful if its data is reliable. Data integrity must be protected by taking precautions to avoid accidental destruction, modification or disclosure. According to Robert Courtney, manager of data security and privacy at IBM, the major security problem is incompetence. "Dishonest people will never catch up to the damage done by incompetence," he said.¹⁴ Operator and programmer errors are the main cause of all accidental software loss.

Without a doubt the most common, embarrassing and expensive software loss is program error. Program errors or "bugs" often do not show up until some rare combination of circumstances reveals them. They originate because of errors in logic, coding, problem definition or systems design. At Cape Kennedy a space launching failed because of a program error. The computer symbol equivalent to a comma was accidentally left out of the program and the mission caused the rocket to go far off course and it had to be destroyed.¹⁵

¹⁴ Arnst, p. 5.
¹⁵ VanTassel, pp. 54-55.
Elimination of program errors is primarily dependent on proper test program procedures. If a program blows up or gives nonsense results it becomes obvious that the program is not working. The real danger lies in the situation where the program seems to be running and providing sensible answers but still the answers are incorrect. Thorough checking by the programmer of his logic and the keypunching must be done before the program is submitted for processing. If this is not done the potential for accidental erasure of data or incorrect modification of data is great. Programs should also be tested out with data where the correct answers are known. This means figuring out the expected results before running. Once the program is tested with test data the next step is to test with actual data. Actual data often brings attention to the errors that test data cannot uncover. Programs should have extensive and very comprehensive checkpoints whenever they process. Parallel runs should be used whenever a new system is being implemented. In this way, if errors occur in the new system, the old system is still functioning and can maintain processing.\footnote{Ibid., pp. 55-57.}

Operator error is the second largest software loss. A simple dropping of a disk pack or the erasure of a volume table of contents causes reruns, a necessity to go to back-up data and confusion in the computer room. Most operator errors can be eliminated through tight programming controls. From this a basic programming rule can be drawn: don't leave anything for the operator
that the program can do and be sure the operator is aware of all
instructions needed to run the program. Many times an operator
mounts the wrong day's tape. In one case the program recognized
the error and printed out a message saying so, but the operator
ignored the message and pushed the restart button. This error
was not discovered until month-end processing was completed and
much work had to be re-run. It is not unforgivable for an operator
to mount an incorrect tape but it is unforgivable for a program
to accept it. Operators should not have the capability to override
serious errors. Auditing of the console printout should be done
daily to determine if the operator is misusing the override option.\footnote{Ibid., pp. 61-62.}^17

Intentional destruction, modification or disclosure of data
can occur by an unauthorized individual gaining access to the system
or by personnel (authorized) within a company or system. For this
reason a well-integrated security system should have as a high pri-
ority tight access control. The need for improved access control
is reflected in a report by the U.S. Chamber of Commerce which
states: "After-hours EDP operations are loosely supervised.
Second and third shifts are typically very informal."\footnote{R. F. Thomley, "Another Look at Computer Room Security," Canadian Datasytems, August, 1975, p. 44.}^18

It is estimated that fewer than 6% of all computer centers
in Canada and the U.S. have card access systems, one of the more
prominent means of access control. Most often access control is
often achieved in computer areas by stationing an employee on guard at the only entrance to check authorization of entrants. He might also keep keys for the building and its computer room and require employees requesting a key to sign their name and times of issuance in a log book. At the end of each day he would account for all keys.  

Mr. R. F. Thornley, General Manager of ADT Security Systems, Toronto, describes one of the most sophisticated card access systems.

"Card access systems, by comparison, include plastic, uniquely encoded cards which serve as keys to unlock either all doors, including tape storage areas or even file cabinets containing classified information. In effect the card is a magnetic key and a "keyport," installed beside a door or in a cabinet, is a lock. Insertion of the card into the keyport unlocked the door. The system's advantage is that it usually costs less than a guard service and unlike locks is very difficult to pick or defeat. The plastic cards which include a photograph of the bearer, can also double as employee identification badges."  

Mr. Thornley also notes that card access systems can also have a log-keeping capability which would record when and who enters where in the center. This most sophisticated card access system is comprised of plastic cards, keyports at entrances and a central controller device which records entrances at the moment they occur. When a card is inserted into the keyport its magnetic code is read and transmitted to the control console which prints out its message on hardcopy.

However the card access system does not positively verify the identity of the entrant. The entrant possibly could have stolen

\(^{19}\) Ibid.

\(^{20}\) Ibid.
the card from an authorized person. Two devices appear to have resolved this problem. One is the Identimation hand geometry recognition system which traces the outline of an individual's outstretched hand and compares it to previously stored data on authorized entrants.

The other has been developed by Calspan Technology Products. It is the Fingerspan identification system which uses the basic technology being considered for digitizing the fingerprint files of the Federal Bureau of Investigation. The system scans an individual's fingerprint, digitizes its physical characteristics, matches them against a previously stored digital record and determines if the person should be admitted. It does not require an intermediate ink or powder image to scan the fingerprint. If the person trying to enter is not authorized an alarm is triggered which could notify a guard. The system has many advantages: (1) it is not messy or inconvenient (2) performance reliability is claimed to be nearly 100% (3) time from terminal activation to system response is very fast (4) data on the entry and exit of particular persons may be logged routinely by the system.21

Special considerations must be given to access control for on-line real-time systems. A teenager in 1973 cost Tymshare Corporation $1,850 in computer-time and a lot of embarrassment. The firm had repeatedly given a high school student a demonstration user name three and a half years earlier when he was taking part in a special program for gifted students. They had forgotten to

---

remove the name from the file of valid passwords for users. In the meantime the student's parents installed a terminal in their home because he was encouraged to use his school district's computer free of charge. The password enabled him to logon to the Tymshare system and he spent over two weeks (at Tymshare's $30/hr. rate) playing games on the computer until he was finally caught. He was not arrested because it was the company's mistake.\(^{22}\) Passwords must be periodically re-issued and old ones removed from the file of valid users in order to ensure their reliability. Physical restriction of access to terminals is plain common sense. More terminals than are needed should not be installed and they should be put in locations where unauthorized users cannot get to them. The security routines in the system should monitor terminal activity to prepare a log of unusual activity and to take action if all is not well. Repeated logging errors, for example, may indicate that whoever is at the terminal is using trial and error to find the right password or log in procedure. There should be some way of identifying which users were resident at any particular time. A usage log should be produced at regular intervals for human inspection.\(^{23}\) More considerations are given in Appendix I.

To protect data from unauthorized individuals, files can be classified into four levels: (1) RESTRICTED, available only to staff and authorized outsiders (2) CONFIDENTIAL, available only to author-


\(^{23}\) Corder, Johnson, Wooleridge, pp. 171-174.
ized staff (3) SECRET, important to company operation, requires special protection (4) TOP SECRET, vital to the organization; requires all-out protection. The user would first have to have his password verified to log in to the system and then to gain access to files the system would also have to verify which files he had access to. 24

The use of systems of secret communication can provide an economical method to increase the security of confidential computerized files. An often overlooked fact is that not only can time-sharing files be protected by cryptography, but many sensitive in-house files can also be economically protected in this manner. The general principle behind the use of cryptographic techniques to protect confidential information is that if unauthorized use is time-consuming and costly, it will be greatly discouraged. A new cryptographic system from Digital Solutions called Safeguard is supposed to secure from unauthorized users any data files used under any 360/370 operating system on a 360/25 CPU or larger. Safeguard encodes user-chosen data fields, including an entire record if desired, according to an algorithm which is selected by specification of a 16-character key. The data is decoded, for use within an application program only if the proper key is specified. 25 Cryptography is probably the most effective means of file and data protection from unauthorized users.

24 Ibid., p. 118.

25 "Safeguard Uses Transient Keys to Code, Decode Data Files..." Computerworld, August 29, 1975, p. 11.
Control of tapes and documentation is another consideration when taking precautions against unauthorized persons. Careful control of copies and tape access should be made. When programs or systems have a market value their worth to the company can exceed their development cost. A library or libraries should exist for the storage and distribution of master documents and tapes.

The authorization procedure used would then depend upon the degree of control and security needed. If this is not great, individuals could get documents and tapes on their own signature. For medium security, the tape or copy might need to be authorized by the team leader, systems manager or other senior person before distribution. Authorization by the data processing manager or managers would give a tighter control.26

Access control can be effectively used to prevent unauthorized users from tampering with the system but how does one prevent fraud by personnel within the system who are authorized employees? For example, in 1970, according to a suit filed in Cook County Circuit Court in Illinois, three operators sold copies of Encyclopedia Britannica's confidential files containing two million customer's names and addresses. The tapes were then sold to mailing houses. The estimated actual loss was in excess of $3 million.

Basically, there are two types of operator fraud: data manipulation and program modification. Source programs and listings should

26 Corder, Johnson, Wolleridge, p. 66.
be inaccessible to computer operators and console printouts should be kept and audited.\textsuperscript{27} Also, if operators duties are related one operator would not be as likely to be able to manipulate data or programs. Programs should be written so they have keys to prevent operator manipulation; that is a correct password is needed before the program will run. A complete checklist for embezzlement and fraud can be found in Appendix J.

Programming fraud and embezzlement involves anyone authorized to instigate program changes—programmers, systems analysts or management. In Washington, D.C., an Internal Revenue Service clerk programmed a computer to list unclaimed tax-refund checks, and had them sent to relatives.\textsuperscript{28} In one bank, a programmer altered a savings account program to transfer the "round off" fractions of cents in the interest calculation to an account he maintained under a fictitious name; he was able to withdraw large sums of money before his scheme was detected.\textsuperscript{29} Prevention of programming fraud and embezzlement necessitates the following controls: library control of programs and documentation; authorization of all program changes; separation of duties and rotation of employees. Library control of programs and documentation provides several forms of protection: (1) Program changes are recorded and restricted to programmers (2) Strict control of programs prevent others from modifying programs (3) Records are kept by the librarian of what program version

\textsuperscript{27}VanTassel, pp. 66-68.

\textsuperscript{28}Strather, p. 146.

\textsuperscript{29}Wasserman, p. 124.
was used for a particular production run (4) Elimination of lost programs (5) Operators should be instructed to delete and load programs which are catalogued on a storage device only on requests from the librarian. If authorization of all program changes is done in a formal manner program integrity will be maintained. Separation of duties means that programmers do not operate the computer and operators do not program to ensure that no one person has complete control of a system. In this way programmers are not able to make unauthorized program changes and run these program changes on the computer without someone's approval. Also, if employees are periodically rotated, no employee or group of employees would be able to so dominate an area of operation that fraud or embezzlement would go undetected. Strict adherence to the rules of library control of documentation and programs, authorization of all program changes, separation of duties and rotation of employees will virtually eliminate the possibilities of programmer fraud or embezzlement.

Because fraud or embezzlement and unintentional error is so difficult to detect, auditing must be done frequently. The auditor no longer has piles of paper to paw through because the computer can be used to do the auditing. Not only should audit aids be provided by the processing programs, but the auditors themselves should have programs of their own with which to audit. The first thing the auditor should do is ask for all the checks he desires in the program, including limit checks, special totals, limits on price changes, etc. The next request should include any
extra printouts desired for auditing purposes. It is essential that as many as possible of these requests are included at the time the original programs were written because if the auditor asks for special program changes after the system is programmed he will probably be told that the change is impossible or will cost too much.

A good auditor will want programs of his own. These programs should be written by someone who is responsible to the auditor rather than the same person who writes the processing programs. A programmer for a large department store decided his girlfriend did not have to pay for purchases from the store that employed him. He simply inserted a routine in the billing program to transfer all charges of his girlfriend’s account to a "dummy" account. He also arranged the program so that when the trial balance was printed, the dummy account did not appear but was included in the total. This fraud continued until the auditor ran a report of his own which indicated the unexplained account. This type of fraud is almost impossible to detect without using special audit programs.30

The internal auditor should have some control of programs to discourage unauthorized program changes. He must have a copy of all necessary programs and receive information on program changes. It would be senseless to have the auditor sit down and check out all program listings because many programs are so long and complicated.

30 VanTassel, p. 49.
Instead of trying to hand check the program, the auditor can create a special set of records and transactions which are processed normally but are used only by the auditor. This allows the auditor to use predetermined tests to ensure everything is being processed correctly. For example, transactions can be constructed so that all program checks and limits are violated and to confirm that edits and checks are working properly. This "mini-company" uses the computer to do the checking. It is particularly advantageous because it permits continuous testing of the system on a live basis. Old-style testing on the computer was forced to use fictitious data or else worry about disturbing actual data but the mini-company is set up independently and can be separated from the real data easily without disturbing the other data.

The auditor should determine which history files should be saved and for how long. He may want special history files kept for his own use and he may be the only one interested in these files. For example, the auditor would want a file of the daily transactions saved on an on-line real-time system. 31

How much security is needed? It is generally agreed that some form of security is needed in every installation and that a mix of safeguards is a good approach. But the amount of protection each user needs depends on the sensitivity of the data, reliability of users and complexity of the system. Consider sensitivity of the data. There is a major difference between an installation processing

31 VanTassel, pp. 50-51.
top secret military information and one processing insurance records. In general, commercial installations do not need to be secured as if they were military camps. Also, there is a big difference in the amount of protection one would put into a computer installation located in the middle of the Detroit ghetto as contrasted with conservative Muncie, Indiana.

Peter Browne wrote in *Computerworld*, February 6, 1974, "...the major factor in providing protection is that of complexity. In today's environment computers are sharing data, programs and systems. They are processing many jobs at once. The greater the extent of resource sharing, the greater the need for security."

There is also a difference in security requirements depending on how much capability is given the user. If the user can only interface with data through a controlled access inquiry system there is less need for protection than if the user is able to write and execute his own programs through a terminal.\(^{32}\)

The passage of the Privacy Act of 1974, which deals with the rights of the individual regarding the federal collection, processing, storage, dissemination and use of information about his personal attributes and activities, put into a new prospective the role of security in the data processing center. A balance must exist between the need for data security and an individual's rights concerning his privacy. The concept of data security should not be used as a basis for continued or extended violations of privacy

\(^{32}\) Peter Browne, "Protection Needs Depend on System's Complexity," *Computerworld*, February 6, 1974.
but should be used to keep personal data confidential and secure from unauthorized access. On the other hand, if limits are not placed concerning the collection of data about an individual, data security could keep one from finding out if his right to privacy has been violated. The balance between data security and privacy is a critical, controversial issue in Congress today and it may be years before the problem is resolved. The issue has made data security a much more vital aspect of the data processing function than it had been previously.

What percentage of the annual budget should go toward the security of the physical plant, processors, storage units, and tape libraries? It is impossible to establish a blanket amount but there are definite criteria on which to base a decision. Robert Courtney of IRM, feels that bringing "risk within tolerable limits at the lowest costs" should be the aim of every user selecting security measures to protect his data center. He feels each security measure's potential benefits should be quantified for comparison with its cost. The two key elements in risk analysis are determining the value of potential loss and the probability of loss. The user must match a potential loss with the probability of it occurring to decide what action to take. The purpose is to identify which of the possible threats would result in the greatest monetary losses, thus developing a guideline to determine what amount of money should be spent to protect against these threats. There are catastrophic events which appear to occur so infrequently that they do not justify

\[23\text{John L. Berg, "Data Security and Privacy: There Is a Difference!", Modern Data, September, 1974, p. 52.}\]
spending large sums to lessen their potential damage. Most often common sense is the best tool in making these risk and probability analyses.34

A data processing center which is very secure from all kinds of potential threats or damage does not necessarily infer that its management has spent exorbitant sums of money on security devices, etc. Basic, common sense measures can be taken which cost nothing. For example, management should screen employees carefully, keeping security in mind and should ensure that basic fire protection rules are followed, etc. If risk is high that a certain catastrophic event may occur, a cost-benefit analyses should be made and all necessary precautions taken to prevent its happening.

Data processing security is a complex, interactive mix of physical, procedural and data protection, with a healthy amount of back-up and audit. As the new generation of computer systems becomes increasingly complex, the need for security rises. Errors are now more costly and harder to detect. A growing reliance of management on information generated by computer systems in such areas as marketing, production, forecasting and engineering has created a greater need for securing the data processing function. It will be up to all of us who have anything to do with electronic data processing—users, systems analysts, auditors, programmers, operators, and management—to maintain the security needed to ensure the reliability and integrity of the data processing function.

APPENDIX A

Fire

1. Install sensors for early detection of heat, smoke, fire.
2. Install wall-mounted or piped extinguishing systems within storage areas and facilities.
3. Rehearse emergency procedures, evacuation and fire-fighting.
4. Maintain direct communication links to central protection agency and/or fire station.
5. Provide fireproof vaults for critical data, tapes, etc.
6. Insist upon proper construction of the facility.
7. Explicit fire instructions must be posted in obvious positions.
8. Combustible materials should be removed from the computer room.
9. The materials used in the false floor, ceiling and computer room facilities should be non-combustible.
10. Store copies of computer files, software, system software, documentation and hardware configuration off the premises.
11. There should be fire detectors and automatic fire extinguishers under the raised floor.
12. Have the computer center checked periodically by a fire expert.
13. Emergency master switches should be near an exit.
14. Areas adjoining the computer area should be well-protected from fire.
APPENDIX B

Flood

1. Water or steam pipes should not be located in the vicinity of the facility or its storage locations.

2. The building should be located on high ground to avoid rising water table or underground stream dangers.

3. Avoid basement and first floor for facility or storage areas.

4. Provide underfloor water drainage.

5. Provide plastic equipment covers for ready access.

6. Seal ceiling and walls against water drainage from floors above.
APPENDIX C

Power Loss

1. Preference is for uninterruptible power supply.
2. Voltage regulators should be used to monitor and control fluctuations.
3. Provide back-up power source (battery or natural gas generator, for example).
4. Locate site in priority service area.
5. Consider power lines from more than one source.
APPENDIX D

Sabotage

1. Remove signs identifying the location of the facility or storage areas.
2. Maintain good control of access to the computer room.
3. Discourage unions or negotiate no-strike contracts.
4. Arrange for and train an alternate work force.
5. Arrange stand-by supply methods.
6. Arrange stand-by transportation for essential staff.
7. Ensure discreet actions and conversations among staff and personnel.
8. Maintain staff loyalty and competence.
9. Conduct pre-employment investigations.
10. Expect "revenge" from disgruntled employees.
APPENDIX E

Eavesdropping

1. To prevent documents or program listings from casually being picked up or copied enforce a clean desk policy and effectively control classified data.

2. Sensitive documents should be shredded when they are of no further use.

3. Typewriters or terminals which overwrite their own ribbon should be used.

4. Prohibit cameras on the premises.

5. Site terminals away from windows to prevent eavesdropping using telescopes or cameras with long-focus lenses.

6. Use cryptography to prevent wiretapping.

7. To prevent electromagnetic eavesdropping use physical measures such as screening, grounding metal objects that carry the radiation and filtering power lines.

8. Have the premises checked for hidden microphones, transmitters or electromagnetic bugs by a security specialist.
APPENDIX F

Programmer Error

1. The programmer should check his program for keypunch errors.
2. The program should provide bookkeeping records such as sequence checking, card counts, record counts, etc.
3. The program should check for the reasonableness of the data.
4. The program should work for all possible conditions such as one transaction.
5. A separate time should be provided for testing the program.
6. Both test and actual data should be used for testing the program.
7. Parallel runs should be used on program revisions.
8. Standards should be used for documenting and programming.
9. A formal policy should be established for program changes.
10. Programmers should be encouraged to write simple easy-to-read programs avoiding tricks, etc.
11. During long-running programs checkpoint recovery should be used.
   A "snapshot" is taken of the collection of data that represents the status at a given time of a program and its peripheral activities.
APPENDIX G

Operator Error

1. Operators should be well-trained and supervised.
2. Programs should check for as many operator errors as possible.
3. Operators should not be able to override error routines.
4. Programs should provide bookkeeping totals that indicate errors such as record counts, reel counts, etc.
5. Computer console output should be saved and periodically checked.
6. Input errors should be resubmitted by a control section.
APPENDIX H

Computer Room Access Control

1. Have a single entrance to the operations area monitored by the receptionist or keep it locked.

2. Continually survey the computer facility and any storage rooms.

3. Install intruder alarms.

4. Install a key lock, a cipher lock or a badge-operated lock on the door to the operations area.

5. Maintain a guard force on 24-hour duty.

6. Use sensors to detect magnets and to prevent them from being brought into the computer center.

7. Locate the operations control room just outside the computer room but adjacent to it.

8. Issue badges with new encoding and change locks periodically.

9. Control use of files through a librarian.

10. Identify all keys to the operations area with a registration number, logged in a control book when issued and marked "Do Not Duplicate."
APPENDIX I

Access Controls for Terminal Use

1. Install terminals in safe locations with locked or guarded entrances.

2. Provide for constant attendance and supervision of terminals during working hours and issue keys to valid users.

3. Design systems so that terminals identify themselves and their operators at the sign-on time, or as requested by the system, or after the system detects that communications have been interrupted.

4. Use cryptography to thwart wiretappers.

5. Use machine-readable cards or badges, which can be issued and collected at each use, to identify terminal users for every job or task performed; change identification cards periodically; and establish procedures for reporting the loss of a card and for taking action.

6. Assign passwords which can be related to authorized codes stored in the computer system.

7. Distribute passwords in a form that can be easily kept and carried by the users, but that cannot be easily deciphered by someone finding a lost password. Change passwords periodically.

8. Inform the personnel who use terminals of their need to prevent unauthorized users from gaining access to the system.

9. Ensure that users sign off before leaving a terminal and that they remove all paper, including carbons and ribbons, which should not be seen by subsequent users.
10. Design systems so that terminals automatically "shut off" if they are left unattended for a specified time.

11. Use techniques such as record counts of input transactions, message verification, sequential numbering of input transactions, and storing of input transactions on tape or disk for future reference along with the data and time of the request, the user's identity, the authorization code, the file accessed and the function performed.
APPENDIX J
Embezzlement and Fraud

1. Source programs and listings should be inaccessible to computer operators.

2. Programs should be inaccessible when not needed.

3. Files should be inaccessible when not needed (stored in a library).

4. Critical programs should be provided with a password so they will run only with the correct password.

5. Console printouts should be kept and audited.

6. Duties should be rotated to prevent an operator or programmer from dominating a file.

7. Operators should not be allowed to re-run programs without authorization.

8. There should always be at least two people in the machine room.

9. Input errors should be sent back to the control section for resubmitting instead of allowing operators to correct errors.

10. Critical forms such as checks should be kept locked up.

11. There should be a formal policy for program changes.

12. Programs and documentation should be controlled by a librarian.

13. The auditor should be informed of all program changes that involve him.

14. Programmer access to the machine room should be tightly controlled.

15. Programmers should be forbidden to run the computer.

16. Operators should not also be used for programming.

17. The manager of programming should develop a plan to protect the integrity of programs.
18. Control final program assemblies so that only the approved program is installed.

19. Periodically compare disk programs to control copies on another medium.

20. Include with output a listing of the job control language to ensure that an unauthorized program has not been executed.

21. Review the software library periodically to ensure that a complete set of source and object programs and operating documentation exists for all applications.

22. Observe employees' work habits.
APPENDIX K

Auditing

1. Auditors should be familiar with the computer operation.

2. The auditor should be involved in the early planning of computer programs. There are many computer checks which, if built in at the time of initial programming, can greatly aid the auditor and help prevent fraud and error.

3. The auditor should suggest checks such as limit checks and special totals which should be included in regular programs.

4. The auditor should have his own programs to double-check files.

5. The auditor should not be dependent on the same programmers who write the original programs for auditing programs.

6. Files should be audited on a surprise basis.

7. The auditor should be promptly informed of program changes.
APPENDIX L

Back-up and Recovery

1. Retain documentation of the old manual system that was replaced by the computer.

2. Examine manual override procedures to see whether they can form the basis of potential fall-back systems.

3. Maintain the capability to produce status listings of vital information.

4. Wherever possible maintain the data preparation activity even if the input is not immediately used to update the master files.

5. Key files should be stored under special conditions to survive any possible disasters. They should also be protected from theft.

6. For tape files the old master file should be kept after each update.

7. A copy of the master should be made before and after each run for disk files since update runs usually replace old records with new ones so that no copy of the old file exists when the run is finished.
BIBLIOGRAPHY


7. __________ "Protection Needs Depend on System's Complexity," Computerworld, February 6, 1974

8. __________ "Reliability Must be Built in, Not Added Later," Computerworld, January 9, 1974.


35. Wilk, Robert J., "Many Measures Exist to Protect Data Integrity...", Computerworld, August 27, 1975, p. 22.
