5-1975

A Study of Computer Security Problems and the Auditor's Responsibility

Gerald L. Titterud

A STUDY OF COMPUTER SECURITY PROBLEMS AND THE AUDITOR'S RESONSIBILITY

by

Gerald L. Titterud

B.A.B.A., Augsburg College 1971

An Independent Study

Submitted to the Faculty

of the

University of North Dakota

in partial fulfillment of the requirements

for the degree of

Master of Science

Grand Forks, North Dakota

May
1975

The writer wishes to express his appreciation to Professor Donald H. Ford and Professor Lyle C. Steinmeier, of the Department of Accounting at the University of North Dakota, for their assistance and suggestions during the preparation of this independent study. He also appreciates the help of Assistant Professor Richard I. Johnson, Chairman of the Department of Computer Science, for his technical assistance and constructive criticism rendered during the preparation of this study.

G.L.T.

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION

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.

Loss through fraud and embezzlement exceeds by a wide margin the total corporate losses through robbery and shoplifting. Opportunities for fraud are enhanced and the problems of prevention are increased with EDP systems because computer-based systems introduce a new list of complications. One basic weakness in most EDP systems is that all of the basic records and supporting details, as well as transaction data and processing programs, are frequently housed in one central location. Previously, fraud attempts would post a more difficult problem because of the necessary dispersal of records throughout many different offices; this particular problem has now been eliminated because all the requisite material is very likely kept in one room.

With the development and implementation of a computer system came the elimination of most of the manual processing. However, also replaced was much of the manual inspection that cannot be duplicated as a part of computer logic. As a result, unusual transactions which in the past would never have escaped detection, now can pass right through the computer system. Accounting records

stored within the system are also vulnerable to manipulation unless properly controlled. The manipulation is difficult to detect because transactions pass through relatively few human hands and may be disclosed purely by accident. Prior to the introduction of EDP, records, transactions, and processes were difficult to change without leaving some telltale mark. Today data files and inputs can be changed almost instantly without leaving a trace. This type of fraud is quite difficult to detect because the false data are in most instances indistinguishable from legitimate data. Also, in most instances, the computer-based systems lack adequate audit trails. In a non-EDP data system, the audit trail consists of journals, ledgers, workpapers, and other documents which permit the auditor to trace transactions backward or forward through the system. In an EDP system, the form, content, and accessibility of records frequently is such that one is unable to follow a single transaction completely through the system.[1]

The auditing of computer-based operations changed dramatically with the introduction of the third generation of computers about five years ago. This new generation permits such things as massive on-line memory banks, multi-processing capabilities, multi-programming and time-sharing with the introduction of segmentation and paging techniques, remote job entry, direct transaction entry, on-line processing and direct retrieval of files from many remote sites, and the centralization and consolidation of information processing and vital corporate information.

Top management's concern about computer security has been stimulated recently by several well-publicized cases of computer related fraud such as Equity Funding, security breaches such as the 1969 and 1970 rash of bombings of computer centers, and natural disasters such as the 1972 tropical storm Agnes which caused wide spread destruction of data centers.[2] This concern is well-founded since any catastrophe of an organization's information system

could and has caused the total collapse of the entire organization. Yet in relatively few companies does one find an all out attack on the urgent problems of computer security and a commitment of appropriate manpower and monetary resources. When profits start to sag, security and control are often times among the first areas to be cut, even with the stakes so enormous.[3]

CHAPTER II

COMPUTER RELATED ABUSES

The opportunities for misuse of a computer system are many and varied, limited only to the imaginations of the engineers and programmers who design these systems, as evidenced by varied types of computer abuse presently on file.

Fortunately, it appears to be rare that the ingenious engineer or programmer who tinkers with the system is bent upon embezzlement. If he did plan a computer robbery with care and patience, he would be likely to succeed. Also, fortunately, the ingenious tinkerer is usually entirely disinterested in accounting. Tally sheets and accounting controls remain a mystery to him. He is preoccupied with his technology. If such a man went into partnership with a financially pressed accountant, the combination could be highly dangerous. It is well to keep them apart.[4]

The combination of talents needed for computer fraud are most likely to be found in the broad-ranging systems analyst or the data-processing manager. It is the latter who is most likely to be able to organize the collusion that would be needed to break into a well planned system. However, the loopholes needed to break into the system may be deliberately designed into it by a systems analyst. This is why it is important to involve the auditors at the design stage.

The programmers who write the software can subvert supposed protective features or install "trapdoors" for subsequent entry. Operators may have daily opportunity to tamper with data or files. Maintenance men may incorporate

subversive instructions into the test programs they employ to test for malfunctions. Wiretaps and various bugging devices can intercept data transmissions or even pick up electromagnetic emanations from wires and terminals. The tappers may use intercepted passwords to "masquerade" as legitimate users, or may even insert their own data into legitimate transmissions. Sometimes legitimate users borrow passwords to masquerade or browse in other people's files. And persons posing as legitimate users may employ a large repertory of tricks to penetrate operating systems from remote terminals.

Especially disturbing is the thought 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. Robert Jacobson, a vice president of Sentor Security Group, Inc., commented jokingly, "Ideally, the first step in securing a system would be to shoot the programmers."[5]

Donn Parker, a senior information processing specialist and researcher at Stanford Research Institute, has recently devoted much time and effort investigating the known cases of computer crimes. He has concluded that ". . . hardly any were discovered through normal security precautions or accounting controls and that nearly all of them were uncovered by happenstance. Some experts estimate that the ratio of undiscovered crimes may be on the order of 100 to 1."[6]

An example of a software manipulation fraud occurred in 1966 in the first Federal criminal case of computerized crime. Software controls are stored in the computer memory where they become invisible and therefore vulnerable to manipulation by the programmer to prevent their use in editing selected transactions. A 21-year-old programmer placed a "patch" (a program change very difficult to detect) in a program used to process bank checks and to detect

overdraft accounts. The patch caused the computer to check to see if the programmer's bank account on magnetic tape was in overdraft. If it was, the computer was instructed to ignore his account when the computer overdraft was prepared. The fraud was finally discovered when the computer broke down and hand calculations revealed the discrepancy.[7]

In 12 cases of computerized bank embezzlement that Donn Parker has analyzed in the late sixties and early seventies, the losses averaged $1,090,000 apiece, or about 10 times the average loss from all other types of embezzlement.[8]

In almost half the recorded cases studied by the Stanford Research Institute, the criminal colluded with someone else, a fact which suggests that theft via a computer often requires more skills and knowledge than is possessed by any one person in the highly structured environment of a computer facility.[9]

There are a number of specific methods used for compromising a computer system, one of the most popular being the "salami swindle." This method is very difficult to detect because only fractional amounts are siphoned off. Such embezzlements usually involve small amounts from many different accounts such as payroll, interest and dividend calculations, stock and commodity trades, or service charge calculations. Who is going to complain if his paycheck is off a penny? But in terms of thousands of such accounts, the pennies add up.

The odds of detecting a "salami swindle" without prescribed security safeguards are minimal, since any losses can be blamed on temporary computer error. Normal accounting controls would stay in balance, unless the perpetrator took a more significant amount from each account.

Computer security has become an even more pressing problem with the development of the online-realtime systems. Online-realtime systems are those in which transactions are processed as soon as they occur and any necessary responses are made immediately. Typically, they involve remote terminals

under the control of the computer. Such systems, coupled with time-sharing and networking make the computerized systems more vulnerable than the traditional processing facilities. Networking involves the linkage of several dispersed computers so that widely separated installations can share data. Time-sharing involves a number of individual users who may simultaneously use a large computer via remote terminals and telephone lines. Because of the speed of the CPU each user has the illusion that his information is being processed immediately.

Such systems utilize techniques that permit the storage of literally billions of characters of data accessible by a computer in less than one second. Via techniques of elaborate methods of segmentation and paging, these systems are able to accommodate and address a huge logical space in comparison to the amount of actual real storage needed. This type of system is essential to provide the necessary catalyst to accommodate many users in an online multi-programming environment.

In order to prevent unauthorized access to such systems, systems commands and passwords have been designed to lock out unauthorized users. Yet these commands and passwords have been easy to obtain from the equipment manufacturer's manuals and trash cans, or from inquiry via remote terminal by programmers masquerading as legitimate users.[10] To date, according to the work done by Rand Corporation and other organizations seeking to improve security in Federal systems, no major defense system has withstood the unauthorized access of a dedicated scheme.[11]

Time-share systems and remote terminals of advanced systems have especially grave potentialities for criminal manipulation. Outside the computer's physical barrier and without fear of surveillance, the clever, computer trained individual can tamper with the system at his convenience, and program the

computer to cover up any evidence that may have existed at the time of the tampering. Consequently, the individual at the external terminal won't provide any of the traditional evidence at the scene of the crime.

Computer misuse and abuse is not necessarily limited to manipulation of system software. An improperly managed computer tape library can lead to costly and embarrassing losses. A client of Ernst and Ernst dispatched $33,000 worth of dividend checks to former stockholders before the error was discovered. The mistake was eventually traced to faulty labeling practices and inadequate programming. Tape reels are externally labeled for coding and identification. In this case the external label was wrong. Proper labeling helps prevent human error. Also, the computer should be programmed to make the final identification. This same type of error has occurred with the processing of incorrect payroll tapes.

Another oversight of a client of Ernst and Ernst involved microfilmed complaints from customers of a leading corporation. The film had been discarded along with the company's regular trash. An enterprising scrap dealer got hold of the microfilm and negotiated its resale to the company for a reported $50,000.

A proper back-up system is always an important element of any well-planned EDP system. There have been a number of instances of sabotage where the contents of magnetic storage devices were destroyed by means of magnetic devices. In one case, data files contained on a magnetic drum were inadvertently destroyed when a member of the cleaning crew attached his magnetic flashlight to the frame of the drum.[12]

In another case, an inexperienced programmer for a client of Ernst and Ernst had made a key change in the accounts receivable file of a major retail store. The change had never been reviewed or tested before running the program under actual operating conditions. This failure was directly responsible for

destroying, by erasure, all accounts receivable. Because proper back-up files were not in existence, this led ultimately to bankruptcy.[13]

There are numerous, clever methods that have been used to defraud computer based operations. A rather simple, yet ingenious, method was implemented by a man who pocketed all the deposit slips at the writing desks of a bank and replaced them with his own electronically coded forms. For three days, every customer who came in without a personal slip and used one of the blank forms was actually depositing money into the culprit's account. The thief thereafter withdrew $100,000 and walked away. He has not yet been found. There are still banks in existence today that use electronic computers, that do not have procedures to prevent this type of computer fraud.

CHAPTER III

COMPUTER SECURITY MEASURES

There are four major areas of security which must be identified and provided for in any computerized information system. These are (1) natural hazards such as fire, water, wind, earthquake, etc., (2) protection of system from destruction by the human element either intentional or unintentional, (3) misuse of the system for purposes of fraud, embezzlement, or personal use, (4) security of the system from industrial espionage or browsing in both company-owned facilities and those used on a time-sharing basis.

In order to provide adequate controls in these four areas, (1) security measures to protect the physical data processing center must be established, (2) organizational controls, (3) administrative controls, (4) hardware controls, (5) software controls, and (6) controls to protect the data files must be implemented.

Physical Facility Security Measures

Location and Site Preparation

Computer security ideally starts with site selection and site preparation. Avoidance of a problem is one of the best protective measures; therefore, the following measures should be observed:

(1) Avoid proximity to airports, gas stations, or other explosion hazards.
(2) Avoid buildings subject to windstorm damage either directly or from adjacent structures.
(3) Eliminate exterior windows in computer rooms.
(4) Avoid lower floors as they have higher exposure to sabotage.
(5) Avoid obvious identifying signs to minimize exposure to sabotage or vandalism.
(6) Good drainage is essential to prevent water damage. Avoid basements.

Avoid locating near water mains. Protect the computer room against water by using watertight seals or by rerouting pipes and conduits.

(7) The building housing the computer site should be protected against external fire damage. Fire walls, fresh-air intakes for air conditioning, and the use of noncombustible structural components are preferable.

(8) Raised floors should be noncombustible material. Under floor drainage is essential. Carpeting in computer areas should be avoided unless fireproof and nonstatic.[14]

Fire Protection

Of the natural disasters, fire is probably the major hazard because of the threat of complete destruction of data files and programs. The reconstruction of destroyed files and programs is very difficult, and often impossible. Insurance figures reflect that approximately one-half of all firms sustaining loss of records through fire are unable to continue in business.

One reason why fire is such a hazard is that computer rooms are typically filled with combustible materials such as paper, punch cards, and printout material. The computer hardware can always be a source of an electrical fire. Sprinkler systems for fire prevention may cause as much damage to equipment and data files as they are intended to prevent.

Automatic carbon dioxide extinguishing systems are recommended for under floor areas, magnetic records, storage vaults, and particularly vital equipment. A disadvantage of using carbon dioxide is that in large quantities in enclosed areas it is toxic to humans, thus demanding a complete evacuation of all personnel.

One of the best fire prevention systems in use today was created by DuPont. Should the detection system sense the presence of either smoke or heat, the computer room is automatically filled with a special gas, Halon R. The gas does not damage the expensive equipment and data files, nor is the Halon system dangerous to operations personnel, and thus permits the staff to remain and carry out emergency procedures.

These emergency procedures should be posted, personnel should be instructed

and fire drills should be exercised periodically.

Protection From Water Damage

As previously mentioned, good drainage is of prime importance to minimize water hazards. While locations above ground level are preferable, it is also wise to avoid top floors and the possibility of roof leaks. Water detection devices are especially useful for under floor areas.

Other protective measures include the installation of pumping systems, use of plastic protective covers for equipment, and sandbags and planks for dire emergencies.

A more subtle source of water damage may result from failure to properly control the humidity on the computer center. High humidity can cause damage to the hardware devices and electrical components.

Protection from Power Loss

A large corporation recently concluded a long and expensive study to determine why its computer system was losing data. Thousands of dollars and many months were spent checking all the hardware and software. The problem was finally traced to the local power company. The utility was unable to supply electrical power within the tolerances specified by the equipment manufacturer for third generation computers.

A recent review of one utility's operations over a twelve month period reported that 10,000 breaker and recloser operations occurred on 231 feeders. However, only 155 of those operations were classed as outages; although every one of the 10,000 would have knocked out an unprotected on-line computer system.[15]

Most third-generation hardware cannot tolerate any power interruption lasting longer than a half-cycle, yet during fault conditions, reclose time of switchgear can be as long as 25 cycles. NASA studies at Cape Kennedy showed that power flickers of less than one-tenth cycle duration can adversely affect

the operations of modern high-speed hardware.[16]

The method in which systems can protect their data integrity is to install a battery-powered uninterruptible power supply (UPS) system as an interface between the power company's power supply and the computer. If the normal AC input from the utility is interrupted, the battery instantly becomes the source of power. The battery can also absorb any voltage surge of the utility or any change in frequency from the standard sixty cycles-per-second.

Control of Unauthorized Access

The extent of the measures utilized to control against unauthorized access are a function of cost versus value. Locked doors are an obvious measure. Door alarm systems, watchmen, desk alarms, photo-electric and sonic alarm systems are more elaborate methods employed.

An excellent security device to prevent unauthorized entrance to the computer room is provided by using a mantrap type of entry system. A person enters the first door using a key or ID card at which time he is viewed and approved by a closed circuit TV before the second door is opened. In more sophisticated systems, the magnetic card reading door locks are connected with a computer so the time, date, and employee number are recorded. Some systems also have magnetic detectors that lock both doors when anyone attempts to bring a magnet into the computer facility or to remove discs or tapes equipped with a very small magnetic strip in the container.

To expand on this type of system, many data processing utilities today employ the use of a network of closed-circuit television cameras. The responsibilities of these utilities are tremendous; one of their major assets being tape files valued at sometimes millions of dollars per file and absolutely essential to the life of the clients they serve.

Many of the larger installations have ruled out the possibility of using

security guards. As one security manager put it:

> If I put on three shifts of guards seven days a week, they would still have to go to the restroom, they'd still see good-looking girls walking by, they'd still get sick, they'd still have to go in and get a cup of coffee or have a cigarette. And there is no way I can afford to meet the payroll necessary to properly control these premises....The cost of this system is less than the cost of one guard's 40-hour-week salary.[17]

The combination of the camera security system plus posted warnings of this complex system has proven to be a major deterrent effect for companies which utilize this system.

Physical Security of Programs and Software

Application programs, operating systems, and the documentation that supports their use should be protected as carefully as any other valuable company asset. The application programs and software must be made available to the operations personnel to fulfill schedules, but with only enough of the system's documentation to do the required work. The console printer log should be reviewed religiously to ascertain that only required programs to perform the scheduled work were used.

All system software and related documentation should be maintained in a fireproof library under lock and key and issued to authorized personnel only upon written authorization. A complete log of issuances from the system's library should be maintained and reviewed by authorized personnel.

Organizational Controls

When an EDP system is utilized, the first step toward preventing collusion is to separate completely the EDP group from the staff who handle the organization's assets. The accountants and clerks will not be permitted to write programs and will not be allowed into the computer room, or any room where data-processing functions take place.

The EDP group should also be functionally independent in its relationship to the departments it serves. Controls should be flexible enough in order to

promote exchanges of ideas and inputs from the user groups so as to retain its service nature to all of the user groups. Such functional independence enhances control by preventing domination of the equipment by any one user.

Another important organizational control is the division of duties within the EDP group. As a very minimum, authority should be delegated so that no single individual is responsible for the complete processing of any transaction. One can safely assume that any programmer or analyst capable of designing and implementing a security system is capable of nullifying its intent. The following procedures are used to minimize computer programming 'weak spots':

(1) Program self-contained, defined modules separately by individual programmers with integration into the total program performed by a senior-type individual.
(2) Program access controls by an outside source.
(3) Employ a subcontractor to evaluate and try to beat the system.[18]

Another cardinal rule is: Don't let the computer programmer actually operate the machine. A crook who can build a loophole into the system and also feed it the data necessary to carry out his bmbezzlement scheme is more likely to succeed than a crook who, after programming the machine, must sit back and hope another operator will innocently let the machine divert funds to him.

It is also a good idea to transfer computer programmers and operators frequently to different machines and different programs. If a crook knows he won't be working on a single job long enough to divert large sums, he's less likely to go to the risk of manipulating the computer to steal, in addition to the fact that the next man on the job might spot the embezzlement procedure.

Administrative Controls

One of the most important controls of any system is thorough documentation of the system. Documentation is difficult and painstaking work, but is absolutely essential for proper and efficient operation of the system. Documentation consists of a definition of the new system, complete system flow-

charts, complete program flowcharts, run manual containing detailed instructions to the operator, listing of Job Control Language, JCL, needed to implement certain procedures, and others depending on the type of system and hardware to be implemented.

The second aspect of administrative control involves program testing procedures applied to new programs. Program testing involves the input of mock data which contain all imaginable values to make sure that the program processes these values as intended. One should keep in mind, however, that there is no known method or mathematical formula which can prove that a program is correct and logical in every conceivable respect.

Hardware Controls As Security Measures

Self-checking numbers

An important form of checking is the use of self-checking numbers. A field that is to be made self-checking has an additional character added to it, which is derived from the other characters by some algorithm. The process is usually applied to numeric fields such as part numbers or account numbers, and one extra digit is added. When an error occurs, the additional check digit is usually not the same as that derived from the other digits and hence reveals that the number is in error.

A common method used to generate a check digit is called the modulus 11 method. The digits of the original number, from right to left, are individually multiplied by the following factors: 2, 3, 4, 5, 6, 7, 2, 3, 4, ... The results are then added. The resulting sum is divided by 11, and the remainder of the division is subtracted from 11. The resulting digit is the check digit, which is attached to the original number to form the self-checking number. This method detects more than 97 per cent of all errors made in keypunching the number, and during data transmission.

Vertical redundancy check - VRC

This hardware method of data integrity is relatively simple and inexpensive. In this method a determination is initially made as to whether there should be an odd or an even number of "one" bits in the binary representation of a character. For instance, using the binary coded representation of the decimal numeral 5, the eight bit representation 00000101 contains two "ones", an even number. Adding a ninth position to the code group, either type of parity may be established.

even parity	000000101	2 "ones"
odd parity	100000101	3 "ones"

If odd parity had been selected a "one" would be placed in the left-most checkbit position. After any movement of data the number of "one" bits is counted and if not an odd number, an error is assumed and processing halted.

Longitudinal redundancy check - LRC

This type of safeguard is used in addition to the vertical redundancy check and is of particular use in data transmission and magnetic tape recording. With this technique, an extra character is sent after some predetermined block of data characters. This extra bit provides parity for its corresponding row similar to the function of the VRC. Obviously, there will be a point of intersection of the parity row column as shown in the illustration. The parity must be predetermined to be correct for one or the other, as it may not be correct for both.

Magnetic Tape

VRC (Odd)									LRC (Even)
	0	0	1	0	0	0	0	0	1	
	1	1	0	0	1	1	0	1	1	
	1	0	1	1	0	0	1	1	1	
	0	0	0	0	0	1	0	1	0	
	0	0	0	0	0	1	0	1	0	
	0	1	0	1	1	0	0	0	1	
	1	1	1	1	1	0	0	1	1	

A limitation of this method is that multiple errors may not be detected during data transmission.[19]

To protect data integrity during processing, several hardware features are available.

Read-after-write

In card punches and magnetic tape drives it is possible to read the data immediately after it has been punched or recorded, in order to compare it with the original data.

Dual read

The card read operation is performed twice and the results compared. Any discrepancies would produce a machine check halt.

Echo

Data transmitted to another peripheral device, a remote terminal, or another computer can be made to generate a return signal which is compared with the original signal to verify correct reception.

Validity check

In any one operating system a particular bit pattern may be unassigned or illegal. In EBCDIC, for example, the number "9" is coded 11111001, but 11111010 is unassigned. A redundancy check would not detect the unassigned bit pattern

as being in error, since both have the same number of "one" bits. However, a validity check would reject the unassigned bit pattern as being invalid.

Similarly, if an instruction word format is being processed, all instructions have a preassigned bit pattern. A validity check would find any unassigned instruction bits and cause a halt in processing.

Interrupts

Interrupts are signals generated by hardware elements that detect exceptional conditions, e.g. parity checks, redundancy checks, overflow conditions, validity checks, etc., and initiate appropriate action. There are five types of interrupts in general use which are vital in maintaining data processing integrity.

Input/output interrupts

An I/O interrupt occurs at the end of an I/O operation, which had been processing simultaneously with the CPU program processing, signalling a request for a change in CPU status from the problem to the supervisor state. As an example a magnetic tape read operation may result in an I/O interrupt caused by a redundancy check as explained previously. In such a case the CPU will change to the supervisor state which will cause the tape to backspace and the data will be re-read.

Supervisor call interrupt

A supervisor-call interrupt occurs when a specific instruction, the supervisor call instruction, is executed by a problem program. The purpose of this instruction is simply to cause a status-switching operation to occur, from problem to supervisor state. Read and write instructions, loading, executing and terminating instructions are examples of functions initiated by supervisor calls.

Program check interrupt

Attempts to use unassigned instruction codes, use of invalid data addresses, or attempts to access protected storage would cause program check-interrupts.

Machine check interrupt

A gain or loss of bits while transferring data from one location to another would cause a machine check interrupt. These types of interrupts are caused by parity errors, or defective circuit modules.

External interrupt

External interrupts are generated by timer action, by pressing an "interrupt" key on the console, or by signals from another computer in a multiprocessing environment.

An electronic clock is generally included in the central processor for recording time of day entries in job logs, and for measuring elapsed time of each job step. This timer acts as an added security measure, preventing sensitive jobs from remaining on the computer long enough to permit unauthorized manipulation of data or instructions.

Internal labeling of tapes

Standard magnetic tape internal labels often include identification numbers, record counts, dates of creation and expiration. These internal labels are computer generated, magnetically inscribed on the tape itself, and automatically checked by programmed instructions.

External ring protection

A hardware interlok prevents writing on any tape in any reel that does not have a ring in its hub. Therefore if a user does not want improper access to a particular tape, he merely has to remove the ring from the hub after removal of the reel from the tape drive.

Software Controls as Security Measures

Input controls

Typical controls implemented within software application programs are dollar controls to check the reasonableness of transactions having monetary worth and quantity controls to check the reasonableness of such applications as sales or inventory transactions to measure units, pieces, and parts. These software controls should be designed to add the quantities, dollar amounts or hash totals and print the totals so that they can be later checked by management for reasonableness. Sensitive calculations should be computed twice by different routines and the results compared to insure accuracy.

Software can be used to validate input, to check numeric fields and alphabetic fields for completeness and integrity, and to test limits on data. It can check codes against tables for validity and check transaction identification numbers against master files for accuracy and validation.

A complete and judicious use of the software controls available can greatly help to eliminate most human errors and any hardware errors.

Output controls

Prior to the release of output reports, the reports should be reviewed for reasonableness and the relationship between the output reports and the console log should be examined. Designated personnel should balance all reports, thereby examining totals of record counts and amounts and relating back to input totals. Proper care should be taken to insure that the correct number of reports are printed and that they are distributed only to the authorized users; any extra copies should be properly destroyed.

All other software controls shall be more properly discussed in the next section on security of data files.

Security of Data Files

One method used to prevent interpretation of data while it is in the form of input data or data on tapes, discs, etc., is to remove its relationship to

other meaningful data, as the removal of field names from input forms and key-punch procedures. A bit of data becomes sensitive only when it is associated with other data, and the more data presented the more sensitive the data becomes.

This same procedure may be used with master files. It may not be advantageous to create a central data bank. It may be wiser to physically separate sensitive master files to eliminate the possibility of relating one file or bit of information to another.

Another security method would be to utilize an algorithm to scramble the data. In scrambling, the data elements are not changed, but their positions within a coding sequence or computer word are changed. Since the actual data scrambling will be done by the computer program when writing out the file, the specific algorithm can be rather complex. The only thing which must be kept confidential is the scrambling technique itself. Once the data is printed on hard copy it is then in a readable form and useable by anyone familiar with the data.

Similar to scrambled data is coded data, which requires actually altering the text characters to coded characters. Again the computer does the coding and decoding, and only when the characters are printed will they be in edited readable form.

Production standard versus actual run times

Actual computer run times should be strictly audited against standard run times to enable management to detect unauthorized computer runs that could possibly generate extra copies of critical reports.

Standard run times should be established for every scheduled production run based upon a reliable volume indicator, such as, quantity of input transactions, records on a master file, or lines of a printed output. The budgeted run times are then compared to the actual run times and variances indicated for management's review. This information is most efficiently accumulated and

reported by system software packages which establish a uniform method of gathering, comparing, and reporting hardware usage versus available hours to establish variances for computer runs, while simultaneously accumulating system performance statistics.

Data security in time-share systems

Data communications between remote facilities via telex and telephone networks carrying millions of bits of data daily is today quite common. These communications systems are quite vulnerable to bugging and wire tapping as a means to break a company's data security. To prevent this type of security breach cryptographic devices have been developed to enable messages to be coded and uncoded to protect data from interpretation. In addition, the telephone companies have devices which can indicate whether wire taps have been made on certain lines.

Computer systems which utilize external terminals in a multi-programming, time-sharing environment, should establish identification and authorization codes to provide a means to protect master files. Tables are generally developed to indicate what an identified user is permitted to do, or which users are permitted to read which records. The table may list for each authorized user items such as the following:

1. Programs that he may use.
2. Types of transactions that he may enter.
3. Data sets that he may read.
4. Data sets that he may modify.
5. Categories of data within a data set that he may read.
6. Categories of data that he may modify.[20]

When a terminal operator indicates the operation he wishes to perform, the programmed security sub-routine checks to see that he is authorized to perform such operations. When a violation is detected the computer can do one of the following things:

1. It can caution the user and give him another chance.

2. It can lock the terminal keyboard and alert security personnel.
3. It can stall the user and at the same time alert security personnel.[21]

The computer should be programmed to produce listings of each day's security-procedure violations and also statistics about them that could rapidly highlight unusual activity. Some systems record not only the procedure violations, but all the requests for sensitive data or all the modifications made to a file. If some doubt about security arises, the security officer can examine this log. The log of file requests may also be analyzed by the computer and statistics produced. The printouts for the security office will highlight periods of unusually high activity on given files. Sudden departures from the norms may be picked out automatically from the activity log, and the security officer will use these to decide whether somebody could be tampering with the system.[22]

Another log should record the actions of the computer room operator. He should never be left free to take any action he chooses with the system. The log should be kept on a locked device so the operator cannot tamper with it. Examination of the log will ensure that he has not inserted his own programs or made use of utility file dumps or other routines that bypass the operating system.[23]

One factor that can help in preventing intrusion into computer systems is that the systems are becoming exceedingly complex. A large amount of knowledge is needed to break into a reasonably protected data bank. One of the principles of safety should be that no one man be able to have all the knowledge that he needs to break into the system. The passwords, authorization procedures, file locks, audit and alarm techniques raise considerably the level of knowledge needed to break into the system. Details of how these facilities work must as far as possible be kept secret, and knowledge of them should be restricted to as small a number of people as possible. Details of the file addressing and control program mechanisms should not be made available to

persons with no need to know. There is a case to be made for an organization designing its own operating system rather than using any that might be available in a computer manufacturer's software. If the design is unique, the workings can be kept secret, whereas anything in a manufacturer's software will be open knowledge.

Contingency Planning and Recovery Techniques

Checkpoints

When something does go wrong it is desirable not to have to repeat the whole of a batch run if it can be avoided. This is especially true when the run is long. For this reason checkpoints are built into the run at appropriately short intervals. If a machine failure occurs or a fault is detected, it is necessary to rerun the work from the last checkpoint, not from the beginning of the entire batch. When a checkpoint is reached, the batch totals up to that point will be recorded along with any other information necessary to restart the run.

File Dumps

A means of massive file reconstruction for files that are directly accessed and overwritten is provided for by periodic file dumps. The input transactions used since the last file dump must also be retained. The files can then be reconstructed by a program that uses the last file dump and the input transaction tapes. Any corrections that may have been made to individual records in the files must be reconstructed also. The program for file reconstruction should be written and tested before the installation is first put into operation. It is during the first weeks of operation that file catastrophes are most likely to happen because of unforeseen program bugs or operators unfamiliar with their jobs.

Emergency procedures

It takes considerable time, money and knowledge to develop a good computer disaster plan. An attempt should be made to quantify risks and costs even if the numbers are very rough. A balance must be established between the need for various kinds of protection, the cost, and the interference with the operation of a system. Qualified outside people, such as the company's auditors, should be involved in developing the plan.

The chief executive of any organization should be given certain basic facts of life before investment decisions are made regarding computer security, if a major catastrophe occurred:

1. Could the organization shut down for a lengthy period of time until adequate computer service was restored?
2. 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?
3. How efficient would your organization be during this recovery period?
4. Would you retain your customers?
5. What would happen to your cash flow?
6. What would recovery cost, if still possible?[24]

There are four major areas of concern to be considered when planning for recovery from a disaster:

1. Arrangements must be made to make available, when needed, particular hardware-software configurations. Duplicate programs and operating instructions are useless unless the company can provide the same computer configuration, including supporting software operating systems, for which they were designed. Since the stresses produced by an emergency situation are not conducive to very effective performance in changing operating procedures and even programs to fit a different computer configuration, arrangements for alternative computers should be made well in advance with frequent review of both the home and alternate systems. Periodic review is important, for the value of a backup plan could be severely limited should the backup computer be changed without proper notification and without corresponding revisions to the backup plan.
2. Operating instructions for the recovery procedures must be carefully documented and stored in a safe area away from the primary installation site.
3. The programs must be copied and stored where they can be properly secured and made readily available when needed.
4. Data files which are essential to continued company operation must be copied and stored in the off-site location. This task, more than any

> other, represents an ongoing, continuing effort. Each time one of these critical files is updated, the off-site backup file must also be updated.[25]

After the disaster plan has been developed and implemented it must be tested. Since people react in emergencies according to the amount of preparation that they have had, periodic drills should be held. Emergency procedures should be well-documented, reviewed by all personnel periodically, and posted in the computer room. All emergency control switches, fire extinguishers, and alarms should be identified by signs or plaque cards and employees trained in their use.[26]

In the event of a computer center disaster, the backup system must be ready to take over in an efficient and orderly manner. To prepare for this situation, a few organizations have conducted computer disaster simulations, and generally, have 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.[27]

There are two basic simulation approaches used: the first involves a series of mock disasters of increasing severity, the second is one large-scale simulated disaster. As deficiencies are uncovered, they are corrected and the exercise continues. The time and money invested in such simulations is very worthwhile according to the organizations who have tried them.[28]

CHAPTER IV

THE AUDITOR'S RESPONSIBILITY

Since the primary function of an auditor is to examine the financial records and express an opinion on them, the techniques and procedures used in an audit are not specifically designed to disclose fraud. If the auditor had to assume responsibility for uncovering all irregularities and defalcations, he would have to extend the scope of his examination to a point where the cost of the audit would be prohibitive. However, the auditor does have a responsibility to examine the internal controls and assure himself that these procedures are adequate and comply with accepted auditing standards. The second standard of field work requires that the auditor must evaluate internal control to determine the type of tests to be taken. Furthermore SAP 33 states, "To evaluate controls, an auditor requires: (1) knowledge and understanding of the procedures and methods prescribed, (2) a reasonable degree of assurance that they are in use and are operating as planned.[29] If an auditor does not review internal control procedures adequately and fraud is subsequently uncovered, he can be held liable through negligence in the performance of the audit.

Internal controls in a manual accounting system are well documented and easy to follow. Records are always visible and a hard-copy record of each transaction is usually available for the auditor to trace through the accounting procedures. With the advent of the computer, however, the auditor is faced with a new situation whereby records are kept on magnetic devices which has eliminated much of the hard copy. Many EDP systems have been developed without the auditor in mind, making it extremely difficult for the auditor to trace any

transactions through the system. Computer technology has advanced faster than the auditing profession has been able to keep up. Also, most systems design engineers and system analysts do not take into account or understand the problems and responsibilities of the auditor in regards to these systems.

These factors have placed the auditing profession in a precarious position. Rule 201 of the AICPA Code of Ethics states: "A member shall not undertake any engagement which he or his firm cannot reasonably expect to complete with professional competence."[30] Therefore, if the accountant conducts an audit and a computer is involved, he by implication states that he is competent to audit the records being produced.

The first general auditing standard stipulates, "The audit is to be performed by a person or persons having adequate technical training and proficiency as an auditor."[31] If the material amounts of a client's accounting data go through the computer, technical competence requires knowledge of computer functions and the potential for fraud by the client's computer personnel. The amount of computer knowledge required by an auditor is currently under debate in the profession. However, the need for technical competence in this area cannot be ignored.

Very few people within the corporate organization or the independent accounting firms possess the required in-depth competency in both areas of accounting and auditing and electronic data processing. Therefore, many companies get started by creating two-man teams consisting of an experienced auditor and a computer technician. Both receive training in the other's area of specialization.[32] All national CPA firms offer extensive in-house training programs to acquaint the auditors with the necessary technical requirements.

Also, a professional organization, EDP Auditors Association, composed of CPA's, internal auditors, and data processing managers, formed in 1969, is concerned with the establishment of standards and control techniques to effec-

tively organize and utilize data-processing resources. Much of the organization's 1974 annual conference was devoted to the auditors' responsibility in preventing and detecting computer frauds.[33]

In order for the auditor to be more responsive to management's desire for a computer system that is sufficiently controlled and fulfills the needs of the auditor, it is extremely important that he participate during the design of the new computer system. The auditor's requirements must be built in at the design stage; they cannot be added on without substantial expense in modifying the programs and system configuration.

A highly automated system can do much of the work of the auditor by enforcing the use of the accuracy checks, security procedures, and balancing controls as discussed previously. The auditors must be present to ensure that the system provides a means for determining that the programs are doing what they were intended to do, and that it also provides a way for the history of individual transactions to be reconstructed.[34]

The auditors should work closely with the development team during testing of the newly created or modified procedures and make sure that the test data are a representative sample. This is very important, for the application may operate much differently during actual operations causing a delay in the implementation.[35]

It is important for the auditor to remember that the system's developers are working against deadlines and severe time and cost constraints; it is the auditor's duty to help them get there on time and in a state of control.[36]

CHAPTER V

RECOMMENDATIONS AND CONCLUSIONS

Recommendations

When first and second-generation computers were introduced into the business community, the audit technique did not change much from that used in manual operating systems, because these computer configurations and operations provided a reasonable level of audit trails and controls.

However, with the advent of third-generation and higher level computer configurations with high-speed multiprogramming, multiprocessing, and large data storage capabilities, the nature of traditional audit trails has changed.

Unfortunately, the auditor has been slow to develop new techniques or approaches to cope with the new environment. The "audit around the computer" approach, in many cases the prevailing practice among EDP auditors, appears inadequate.

EDP auditors should know, understand, and speak the language of computer people. They should be able to understand the mechanics and capabilities of any hardware/software configuration and system control procedures before undertaking an EDP audit in order to determine which applicable and appropriate audit technique to apply. The EDP auditor should have a working knowledge of computer programming systems, teleprocessing, computer operation, job control languages, console messages, Customer Information Control Systems (CICS), etc.[37]

As long as the EDP auditor is deficient in technical skills in these areas, the EDP audit effort will be compromised and generally inadequate.

Accounting curriculums at most colleges and universities do not offer much course work in the area of computer systems due to the four year time constraint. Therefore if the student is interested in EDP auditing, he must arrange for a five year program.

Typically, however, auditors acquire the necessary knowledge through professional development courses and job experience. All of the national firms offer training programs in EDP auditing; or the auditor may wish to gain knowledge in this area by attending night school in order to fulfill his professional development requirements.

It is quite evident that the computer is rapidly becoming an integral part of the audit function, for the term "audit around the computer" will likely become an unacceptable audit technique.

Conclusions

The development of computer hardware and software has progressed much faster than the controls to secure such facilities and techniques to establish internal control and audit procedures for such facilities.

Up to now, computer hardware and software have been designed to maximize computer efficiency and to provide maximum throughput at the least cost. Audits and safeguards have been mostly ignored. Computer personnel have been given maximum flexibility in the design, installation, and control of computer systems.[38]

However, these things are changing for the business community is putting heavy pressure on the computer manufacturers to develop a more secure computer. IBM is currently conducting a five year study to produce sorely needed information on computer controls and security which will cost in excess of forty million dollars for research.[39]

In the next generation of computers, much software, such as operating systems, data management systems, and data communications systems, will be con-

verted into hardware. Software can be easily tampered with, hardware cannot.

And finally, new and improved hardware and software will be developed and used more extensively in order to give better administration and control of the security, the administration, the access to, and the use of corporate data.[40]

FOOTNOTES

[1]John M. Horne, "EDP Controls to Check Fraud," Management Accounting, October 1974, p. 44.

[2]Harold Weiss, "Computer Security an Overview," Datamation, January 1974, p. 42.

[3]Ibid.

[4]James Martin, Security, Accuracy, and Privacy in Computer Systems, (Englewood Cliffs, New Jersey, 1973), p. 408.

[5]Tom Alexander, "Waiting for the Great Computer Rip-Off," Fortune, July 1974, p. 146.

[6]Thomas Porter, Jr., "Computer Raped by Telephone," The New York Times Magazine, September 8, 1974, p. 36.

[7]Ibid., 36.

[8]Ibid., 40.

[9]Ibid.

[10]Ibid., 43.

[11]Ibid.

[12]Paul R. Howes, "The Computer and You," The Practical Accountant, May/June 1974, p. 51.

[13]"Computer Security," Ernst and Ernst, Summer 1974, p. 7.

[14]Arthur E. Hutt, "Management's Role in Computer Security," in Computer Security Handbook, ed. Douglas B. Hoyt, Darwin M. Ley, Stephen F. Piron, and John K. Roth, (New York, 1973), p. 47.

[15]"Uninterruptible Power Supply (UPS): A Watchword," Infosystems, August 1974, p. 28.

[16]Ibid.

[17]"Security Through Snooping," Infosystems, September 1973, p. 84.

[18]Dr. Thomas V. Sobczak, "Information - Your Company's Greatest Asset," in Computer Security: Equipment, Personnel, and Data, (Los Angeles, 1974), pp. 33 & 34.

[19]Seymour Bosworth, "Hardware Elements of Security," in Computer Security Handbook, ed. Douglas B. Hoyt, Darwin M. Ley, Stephen F. Piron, and John K. Roth, (New York, 1973) p. 47.

[20]Martin, p. 159.

[21]Ibid., p. 179.

[22]Ibid., p. 184.

[23]Ibid.

[24]Weiss, p. 44.

[25]Dr. Elise G. Jancura, CPA, James J. Nance, Jerolene A. Drefs, "What to do before Your Computer Blows Up," Computers and People, February 1974, p. 16 & 17.

[26]Ira S. Gottfried, "Protect or Perish," Data Management. September 1973, p. 25.

[27]Weiss, p. 46.

[28]Ibid., p. 47.

[29]Eugene H. Kramer, "Computers add new dimensions to accountants' legal liability," Practical Accountant, March/April 1974, p. 46.

[30]Ibid.

[31]Ibid.

[32]Leighton F. Smith, "The Internal Computer Audition: One Answer to Computer Misuse," The Arthur Andersen Chronicle, January 1974, p. 9.

[33]Porter, p. 41.

[34]Martin, p. 414.

[35]Fenwicke W. Holmes, "Auditing from the DP Manager's Viewpoint," Journal of Systems Management, p. 25.

[36]Ibid.

[37]Gabriel G. Tashji, "DP Auditor Limited by Lack of Knowledge," Computerworld, April 9, 1975, p. 14.

[38]Smith, p. 14.

[39]Herbert E. Dickson, "Software Controls and Security," in Computer Security Handbook, ed. Douglas B. Hoyt, Darwin M. Ley, Stephen F. Diron, and John K. Roth, (New York 1973), p. 75.

[40]Ibid.

BIBLIOGRAPHY

BOOKS

Bosworth, Seymour. "Hardware Elements of Security." In Computer Security Handbook. Ed. Douglas B. Hoyt, Darwin M. Ley, Stephen F. Piron, and John K. Roth. New York: Macmillan Publishing Co., Inc., 1973. Pp. 44-61.

Dickson, Herbert E. "Software Controls and Security." In Computer Security Handbook. Ed. Douglas B. Hoyt, Darwin M. Ley, Stephen F. Piron, and John K. Roth. New York: Macmillan Publishing Co., Inc., 1973. Pp. 75-85.

Hutt, Arthur E. "Management's Role in Computer Security." In Computer Security Handbook. Ed. Douglas B. Hoyt, Darwin M. Ley, Stephen F. Piron, and John K. Roth, New York: Macmillan Publishing Co., Inc., 1973. Pp. 1-14.

Jones, Ralph E. "Data Files." In Computer Security Handbook. Ed. Douglas B. Hoyt, Darwin M. Ley, Stephen F. Piron, and John K. Roth. New York: Macmillan Publishing Co., Inc., 1973. Pp. 62-74.

Martin, James. Security, Accuracy, and Privacy in Computer Systems. Englewood Ciffs: Prentice-Hall, Inc., 1973.

Menkus, Belden. "Computer Facility Physical Security." In Computer Security Handbook. Ed. Douglas B. Hoyt, Darwin M. Ley, Stephen F. Piron, and John K. Roth. New York: Macmillan Publishing Co., Inc., 1973. Pp. 15-26.

Sobczak, Dr. Thomas V. "Information-Your Company's Greatest Asset." In Computer Security: Equipment, Personnel, and Data. Ed. June Elizabeth Thorsen. Los Angeles: Security World Publishing Co., Inc., 1974. PP. 29-34.

PERIODICALS

Alexander, Tom. "Waiting for the Great Computer Rip-Off." Fortune, July, 1974, Pp. 143-154.

Anderson, Dr. Lane K. "Self-checking digit concepts." Journal of Systems Management, September, 1974, Pp. 36-42.

Autry, Vaughn M. "Computer: Boon or Downfall." Data Management, January, 1974, Pp. 26-29.

Baird, Lindsay L. "Identifying Computer Vulnerability." Data Management, June, 1974, Pp. 15-17.

Bigelow, Robert P. "Opportunity makes a thief." Infosystems, February, 1974, Pp. 24-28.

Buckland, Gerald L. "Aftermath of a Flood." Data Management, January, 1974, Pp. 10-13.

Caffrey, J. J. "Protecting Computers." Datamation, October, 1973, Pp. 94 & 95.

Carlton, John M. "EDP Controls to check Fraud." Management Accounting, February, 1974, Pp. 33-36.

Campaign, Howard. "Computer Privacy and Security." Computers and Automation, July, 1973, Pp. 12-17.

Chastain, Dennis R. "Security vs. Performance." Datamation, November, 1973, Pp. 35-39.

"Computer Security." Ernst and Ernst, Summer, 1974, Pp. 2-9.

"Computer Security - the imperative nuisance." Infosystems, February, 1974, Pp. 24-28.

"Computer Theft History: Case Of The 6 Second Tape." Data Management, August, 1973, p. 41.

Devlin, Gerald W. "EDP Security Control." The Internal Auditor, July-August, 1974, Pp. 16-25.

"Fire Protection." Data Management, January, 1974, p. 19.

Gellman, Dr. Harvey S. "Using the Computer to Steal." Journal of Systems Management, October, 1974, Pp. 28-32

Gottfried, Ira S. "Protect or Perish." Data Management, September, 1973, Pp. 23-27.

Holmes, Fenwicke W. "Auditing from the DP Manager's Viewpoint." Journal of Systems Management, March, 1974, Pp. 22-25.

Horne, John M. "EDP Controls to Check Fraud." Management Accounting, October, 1974, Pp. 43-46.

Howes, Paul R. "The Computer and You." The Practical Accountant, May/June, 1974, p. 51.

Huemer, David A. "Recovery and Restart In a Real Time System." Data Management, September, 1973, Pp. 61-67.

Jancura, Dr. Elise G. "EDP-Computers and Auditing." The Woman CPA, January, 1974, Pp. 13-15.

Jancura, Dr. Elise G. "What to do Before Your Computer Blows Up." Computers and People, February, 1974, Pp. 16, 17.

Korodi, Miklos B. "Computer Room Security." Data Management, January, 1974, Pp. 15-17.

Kramer, Eugene H. "Computers Add New Dimensions to Accountants' Legal Liability." Practical Accountant, March-April, 1974, Pp. 46 & 47.

Menkus, Belden, "Computerized Information Systems Are Vulnerable to Fraud and Embezzlement." CPA Journal, July, 1973, Pp. 617-619.

Menkus, Belden, "What management can do about fire in the EDP center." Administrative Management, August, 1974, p. 14.

Palme, Jacob. "Software Security." Datamation, November, 1973, Pp. 110, 111, 116.

Parker, Donn B. "Computer Crimes." The Office, August, 1973, Pp. 43-47.

"Physical Security in EDP-an Overview." Journal of Accountancy, June, 1974, Pp. 46, 48 and 49.

Porter, Thomas Jr. "Computer Raped by Telephone." The New York Times Magazine. September 8, 1974, Pp. 33-43.

Scoma, Louis Jr. "Computer Security." The Office, August, 1973, Pp. 48 & 49.

"Security through snooping." Infosystems, September, 1973, Pp. 84 & 85.

Smith, Leighton F. "The Internal Computer Auditor: One Answer to Computer Misuse." The Arthur Andersen Chronicle, January, 1974, Pp. 8-14.

Sobczak, Dr. Thomas V. "Information - Your Company's Greatest Asset." In Computer Security: Equipment, Personnel, and Data.

"Software Security." Journal of Systems Management, September, 1973, Pp. 18-23.

Stern, Ludwig. "Contingency Planning: Why? How and How Much?" Datamation, September, 1974, Pp. 83,87,89,91,93,95.

Stone, Robert L. "Computer Abuse." Journal of Accountancy, February, 1975, Pp. 35-39.

Tashji, Gabriel G. "DP Auditor Limited by Lack of Knowledge." Computerworld, April 9, 1975, p. 14.

Thorne, Jack F. "Control of Computer Abuses." Journal of Accountancy, October, 1974, Pp. 40-46.

"Uninterruptible Power Supply (UPS): A Watchword." Infosystems, August, 1974, p. 28.

Weiss, Harold, "Computer Security: an Overview." Datamation, January, 1974, Pp. 42-47.

Yasaki, Edward K. "A New Science Emerges: Plugging The Holes in Operating Systems." Datamation, February, 1974, Pp. 90-92.