



5-1-1989

## A Management Perspective On The People, Procedures And Prevention Of Computer Crime

Lt. James B. Roan

Follow this and additional works at: <https://commons.und.edu/theses>



Part of the [Business Commons](#)

---

### Recommended Citation

Roan, Lt. James B., "A Management Perspective On The People, Procedures And Prevention Of Computer Crime" (1989). *Theses and Dissertations*. 4424.

<https://commons.und.edu/theses/4424>

This Independent Study is brought to you for free and open access by the Theses, Dissertations, and Senior Projects at UND Scholarly Commons. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of UND Scholarly Commons. For more information, please contact [und.common@library.und.edu](mailto:und.common@library.und.edu).

A MANAGEMENT PERSPECTIVE ON THE PEOPLE, PROCEDURES  
AND PREVENTION OF COMPUTER CRIME

by

Lt James B. Roan

Bachelor of Business Administration, University of Oklahoma, 1986

An Independent Study

Submitted to the Graduate Faculty of

The University of North Dakota

in partial fulfillment of the requirements

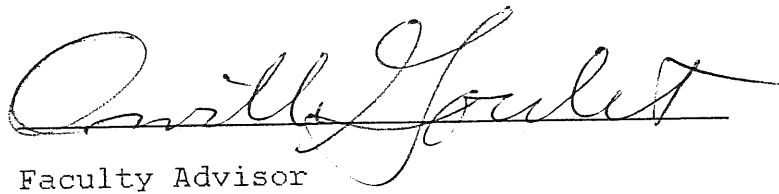
for the degree of

Master of Business Administration

The University of North Dakota Graduate Center

May  
1989

This independent study submitted by James B. Roan in partial fulfillment of the requirements for the Degree of Master of Business Administration from the University of North Dakota is hereby approved by the Faculty Advisor under whom the work has been done. This independent study meets the standards for appearance and conforms to the style and format requirements of the Graduate School of the University of North Dakota.



Corinne Foulet

Faculty Advisor

## ACKNOWLEDGEMENTS

Due to the encouragement and support of many people I was able to complete this project.

First, I thank my wife, Michelle, who offered assistance when I needed it, and kept me going until I finished.

Secondly, thanks to Dr. Orville Goulet for his advise in making this paper a worthwhile accomplishment.

Lastly, thanks to all my professors and fellow students who made the MBA program an enjoyable experience.

## ABSTRACT

A Management Perspective on the People, Procedures, and Prevention of Computer Crime.

James B. Roan, BBA

Faculty Advisor: Professor Orville Goulet

The area of computer crime is a new and complex one. Corporations are increasingly feeling the ramifications of computer crime. It is estimated that computer crime has an impact of over four billion dollars yearly.

The types of computer crime include vandalism, theft of industrial secrets, and theft of financial assets. The range of computer crime includes profit organizations, service centers, and research facilities. A new danger for research and medical centers is the possibility of destroying vital research data.

The type of people involved in computer crime are varied. Most of the people are not super intelligent; rather they are people who have had an opportunity to use the computer and understand ways of circumventing computer safeguards. The most common abuser is the company employee who uses his or her position and has the skill, knowledge, and access. There are numerous methods of entering the system; including data diddling and the trojan horse technique.

Because of the rise in computer crime, there has been a need to upgrade security systems. Until recently, the gap between computer technology and security technology has been

increasing. New innovations have started to add more security to the system. New computer systems must have the capability to be upgraded as the techniques of computer crime improve.

There has also been a push to get legislation passed aimed at slowing down computer crime. Because the area of computer crime is new, it is taking time to implement the laws. The courts are also having to approach the area slowly. There are few cases pertaining to computer crime, so many of the cases now in court are setting precedents.

The purpose of this study is to enlighten managers and users of computers on the need for a secure system. There are a number of useful policies and procedures which can be implemented to keep computers and their assets safe.

increasing. New innovations have started to add more security to the system. New computer systems must have the capability to be upgraded as the techniques of computer crime improve.

There has also been a push to get legislation passed aimed at slowing down computer crime. Because the area of computer crime is new, it is taking time to implement the laws. The courts are also having to approach the area slowly. There are few cases pertaining to computer crime, so many of the cases now in court are setting precedents.

The purpose of this study is to enlighten managers and users of computers on the need for a secure system. There are a number of useful policies and procedures which can be implemented to keep computers and their assets safe.

## TABLE OF CONTENTS

ABSTRACT .....	iv
CHAPTER 1. INTRODUCTION .....	1
CHAPTER 2. IMPACT OF COMPUTER CRIME ON INDUSTRY .....	4
CHAPTER 3. METHODS OF COMPUTER CRIME .....	9
CHAPTER 4. THE PEOPLE INVOLVED .....	18
CHAPTER 5. RISK ASSESSMENT .....	22
CHAPTER 6. SECURITY PROCEDURES .....	29
CHAPTER 7. MANAGEMENT RESPONSIBILITIES .....	39
CHAPTER 8. LEGAL CONSIDERATIONS .....	45
SUMMARY .....	50
BIBLIOGRAPHY .....	53



CHAPTER 1  
INTRODUCTION

PURPOSE OF STUDY

The objective of this paper is to examine the various types of computer crime and identify the methods by which management can protect their computer resources. The study will look at previous examples of computer crimes, the people involved, the methods for detection and prevention, management's responsibilities and finally the legal issues which are involved. The thrust of the paper will deal primarily with the concerns of business managers, although it is relevant to any industries which utilize computers.

The area of computer crime is a new and increasingly important subject for managerial concern. Corporations are continually feeling the ramifications of theft which come from computer abuse. Billions of dollars are lost yearly. This loss is not only in the form of money, but also assets, information, industrial secrets and privacy are all subjected to computer abuse.<sup>1</sup> The senior management of companies must realize that their computer systems are vulnerable to "attack" and precautions must be taken. Because computers are a new and complex field, many managers are uncomfortable and have little knowledge of how computer systems operate. They have even less knowledge of the methods

-----  
<sup>1</sup>  
Michael Thomas, "Rise in Computer Oriented Crimes,"  
National Underwriter, 1 August 1984, pg. 35

that are used to commit crimes by computer or in ways to prevent them. The thrust of this study will be to educate and inform managers of business on the effects of computer crime and means to combat it.

#### LIMITATIONS OF THE STUDY

There are certain constraints associated with this study. One of the most important is disseminating the vast amount of information which is available on the subject of computers and computer crime. Computers are a highly technical field, and there are numerous methods for examining how they operate and what they can be used for. The knowledge of how computers can be used is increasing at a fantastic rate. Children in grade school are learning with hands on experience how to operate computers. This increase in knowledge is bringing about new ways to manipulate computers for both positive and negative purposes. With respect to computer crime, 14 year olds are capable of bypassing elaborate security system and altering sensitive documents. For each new security system developed, a new way to get around it is created. Herein lies the limitation. It is impossible to fully cover every aspect of computer crime. What this study is designed to do is inform managers of what they must be on the look out for. They must be made aware of means of protection of valuable resources and understand how previous examples of this new form of white collar crime can be used to reduce instances of crime in their own companies.

## METHODOLOGY

This study will research the existing literature which is available on computer crime and its prevention. Text books, research books, periodicals, and personal interviews are utilized to gain an understanding of this new and complex field of study.

## CHAPTER 2

### IMPACT OF COMPUTER CRIME ON INDUSTRY

In the last 40 years the world has been through a technological revolution. One of the driving forces behind this movement is the creation and use of the computer. Computers, which a few years ago were scarce and expensive, are now abundantly found in homes, schools and business. Business is rapidly becoming dependent on the capabilities that computers provide. Companies rely on the computers for inventory control, payroll management, and assembly processing to name but a few. As a result of this increase in use, and an ever increasing knowledge of computer systems, the newest form of white-collar crime has appeared - computer crime.<sup>2</sup>

One definition of computer crime according to the Justice Department is that computer crime is "any illegal act for which knowledge of computer technology is essential for its perpetration, investigation, or prosecution."<sup>3</sup>

Computer crime has increased due to the availability and access to computers. Anyone with sufficient knowledge of computers can commit a computer crime. There are several examples of misusing computers for personal gain:

-----  
2

Interview with Professor Leon Price, University of Oklahoma, 26 March 1985

3

Dorothy B. Francis, Computer Crime, (New York: E.P Dutton, 1987), 1.

In 1972, a student was arrested for stealing more than \$1 million in electronic equipment using only a modem and a computer access code which he obtained by watching employees. He was caught only because a co-worker turned him in.

In Milwaukee, a group of young computer enthusiasts managed to bypass security systems at a national defense installation, gaining access to vital military secrets.

While these are but a few of the hundreds of different types of computer crime, they are representative of everyday people using computers for illegal purposes.

The cost to business is staggering. The loss due to computer theft is estimated to be one to four billion a year and rising rapidly. Many experts feel that this number is greatly underestimated. They say that the number is not accurate because many companies are unaware that their computer system is being tampered with. Corporate managers are also very hesitant to admit that their assets are being stolen without their knowledge. Such an admittance could tarnish their reputation. They fear that the public opinion would be that they cannot responsibly manage their business. Many organizations make the decision to ignore the loss or take care of the problem without the public becoming aware. Such tactics force the company to pass along the loss from computer crime to the consumer. Thus, the consumer is

-----  
4

Interview, Price.

5

"Computer Crime Hits Hard." OECD Observer, April 1984, pg. 36-39.

charged greater amounts due to the negligence of the company. The actual occurrence of a company reporting a computer crime is only estimated to be five to ten percent. The remaining 90% is not reported.

The response by business to computer crime has been very slow. In a survey of 200 companies, only 70% of the Data Processing Management Association feel there is a need for security. Only 65% make some sort of allocation in their budget for computer security. Many of these companies have an overinflated sense that their computer systems are invulnerable and no one can gain access to them. When the average computer theft is estimated to be \$450,000, it is unwise thinking to take inadequate security measures.

Companies have numerous regulations and procedures for purchasing computers, but have almost no established procedures for securing them. Why do companies procrastinate on computer security? Four theories have been proposed to answer this question.

- (1) Computer crime is bad publicity for the company.
- (2) Only 1 in 10,000 computer crimes are prosecuted.
- (3) Managers do not understand the type of security to be implemented.
- (4) The perceived high cost of security

-----  
6

"Computer Fraud", Management Today, 2 September, 1983, pg. 24.

7

"Computer Crime Hits Hard", OECD Observer p. 19.

8

Richard H. Baker, The Computer Security Handbook (Blue Ridge Summit: Tab Books Inc. 1985), pg. 8.

As mentioned before, companies will do all they can to avoid bad publicity. Instances where a corporation losses millions of dollars from illegal electronic transfers do not gain much support from the stockholders. They often will hide the event, trying to keep any information from leaking out. To incorporate a multi-million dollar security system might bring adverse implications to the company by admitting defeat.

The legal implications associated with computer crime are still in their infancy and few if any people are prosecuted. Reasons for this range from being too highly technical for the prosecution and courts to understand, to loopholes which are available for criminals to use. Congress has been slow in reacting to computer crime.

One of the largest problems in detecting computer crime lies with the management of companies. Many high and mid-level executives do not understand the complexities associated with computer systems. They leave the applications of the computer to the technical employees. Subsequently, the managers who need to make definitive procedures and policies on the proper use of computers have little understanding of the system. Without high-level backing, computer security systems are doomed to fail. Management must make the effort to support a useable computer security system in terms of money and technical assistance.

One of the final reasons that companies hesitate to use

security systems is the perceived cost of the system. Some highly technical systems are expensive and costly to use. Computer security can consist of nothing more than entry procedures and passwords; methods which cost practically nothing and can be obtained from any computer catalog. The loss that can be associated with computer crime often outweighs the cost of securing it.

Effective security management can only come when a concerted effort is made between each division of the company. Security of computer systems requires a full-scale investigation into the possible weak areas where computer fraud can be conducted. A knowledge of the common methods of computer crime, the suspects to look for if fraud occurs, a realistic risk assessment of the company, means of securing the system, and most important, the management policies and procedures to be used are essential for a company to protect its equipment and data. The following chapters will deal with each of these sections and will assist managers in keeping their computer systems safe.



## CHAPTER 3

### METHODS OF COMPUTER CRIME

There are numerous ways for computer crime to be accomplished. As the knowledge of computers increases, the ability of people to undermine the security systems also increases. The methods of computer crime are continually changing, however, there are some standard methods that have been used in the past. Managers must continually monitor their systems for evidence of illegal use. The following illustrations identify the most common forms of abuse, and gives certain controls that management can use to help prevent their occurrence.

#### PHYSICAL ABUSE AND NATURAL DISASTERS

Physical abuse deals with the actual destruction of the computer system or its peripheral equipment. Numerous examples have occurred where a disgruntled employee or customer has destroyed a company's computer system by burning, shooting, bombing or even putting an axe to it as a way of "getting revenge". Destruction of the equipment is not the only way in which a system can be damaged. Loss of data can handicap a company as much or even more. The time to replace the lost financial or marketing data can take weeks to months. Destroying floppy disks and hard drives, using strong electromagnetic fields, identity loss, and logical damage are some of the common forms of data mutilation.

Obviously, in order to make a physical attack on the computer system, the person must have access. It is here that the manager can reduce the risk of physical attacks. Controls on physical access, site hardening, backups, and recovery planning are the best means of protection.

Physical access controls include fences, guards, electronic alarms, and entry barriers to the computer rooms. The newest security measures available require the person requesting entry to verify his authorization through a physical characteristic such as fingerprints, retina pattern, or even weight distribution. While these methods are still new and imperfect, they are providing better control to the access of the computer system.

Other methods for managing physical attacks include separate heating, air conditioning, uninterruptable power supplies, and fire fighting equipment designed for computers. While expensive, the amount saved through this protection can help to offset the cost that would occur if a companies computer system or storage facilities were destroyed.

Natural disasters involves damage to the system through means other then overt. Occurrences such as tornadoes and earthquakes are examples of large-scale disaster. Although it is impossible to prevent such incidents, it is possible to

establish procedures for dealing with them. Computer centers should be kept away from areas with a high risk of natural disaster. Even more importantly, a company's backup records should be kept well away from its main center to insure they can recover their files if they are lost. Equipment can also be hardened to help minimize the effects of large scale storms.

Besides acts of GOD, there are other forms of "natural" destruction. The effects of extreme temperature, excessive amounts of dust or smoke, spilling of liquids, static electricity, and even living organisms (rodents and insects) can severely hamper the operation of a computer system. Again, while impossible to completely remove all these threats, it is possible, through effective management techniques, to minimize their effects. Stated policies and procedures must be implemented and enforced which prohibit actions which would adversely affect the system. For example, a typical policy prohibits bringing in any drinks or food into the computer room. Likewise, smoking is strictly prohibited because a single smoke particle can ruin a read-write head. These policies must be the responsibility of the manager in charge, but they must be enforced by every employee.

There are numerous examples of a overt force causing the destruction of a computer. In 1970, a bomb was planted in

the University of Wisconsin Math Research Center. One person was killed and over 20 years of research and \$16 million in research investment was lost. No contingency plans for backup files had been created.<sup>12</sup>

### DATA DIDDLE

Data diddling is considered to be the "simplest, safest, and most common method used in computer crime."<sup>13</sup> It involves the unauthorized changing of data before or during input to the computer system. The data changed can be anything from a customer's name, to forging or counterfeiting documents. It can be very difficult to pinpoint the culprit because numerous people have access to the computer. The most common abusers are employees who enter data into the computer. Data bases may have thousands of entries, and a change to one record is very difficult to detect.

Various managerial controls include audits and internal checks of the system to insure that unusual data which is entered is flagged and can be checked. Rotation of employees and forced vacations may cause different results or results which should not occur, i.e. overtime to that person.<sup>14</sup>

12

Francis, Computer Crime, pg. 8.

13

Adrian R. D. Norman, Computer Insecurity (New York: Chapman and Hall. 1983.), pg. 90

14

Donn B. Parker, Computer Security Management (Reston: Reston Publishing Company Inc. 1981.), pg 230.

One case example occurred in 1973, when the top management of the Equity Funding Corporation of America were convicted of creating false "lives" to sell to reinsurers. More than 20 people were convicted of federal crimes. Shareholders lost \$600 million and policies were lost amounting to \$1 billion.

15

### TROJAN HORSE

A trojan horse is the improper placement of computer instructions in a program so that the computer will perform unauthorized routines, but usually still allow the program to run as usual. The Trojan Horse is most often used to insert a logic bomb or computer virus into the central processing unit. Detection can be very difficult. The illegal routine can be hidden in millions of lines of program. One possible means of detection for a trojan horse is to run the operating program against a master program at unscheduled times to see if any changes can be noticed.

16

### SALAMI TECHNIQUE

This form of computer theft takes very small amounts of money from large bank accounts and multiplies the amount by thousands of similar accounts. No alarms or flags are set off by this type of crime because the accounts, which are still correct, reflect the proper amounts of funds. For example, if

-----  
15Norman, Computer Insecurity, pg 119

16

Parker, Computer Security Management, pg 231

the interest payment on an account equates to \$91.43255, the salami technique will take the additional .00255 cents and place it into a separate account. This amount is then added to hundreds of others accounts. The illegal account quickly grows into thousands of dollars. Detection is difficult. Auditors see that all accounts are balanced and there are no complaints from customers. One of the few ways of determining if a salami technique is being used is to see if any employees have sudden changes in their financial status, or if the maintainers are spending an unusual amount of time working on the computer. Rotation of employees will help to reduce this occurrence.

17

One employee maintained his fraudulent account for years under the name of Zzwicke. He was only discovered when the bank ran a promotion contest and gave prizes to the first and last customers on the list.

18

### SUPERZAP

The superzap is a utility program which has legitimate uses. The program allows the user to override existing security measures. It is a type of skeleton key which lets the user bypass security systems and have access to areas they could not have accessed with normal procedures. The program

-----  
17

Donn B. Parker, Crime By Computer (New York: Charles Scribner's Sons. 1976.), pg. 114

18

Norman, Computer Insecurity, pg 83.

is used to fix problems which occur in the computer system and cannot be corrected with normal diagnostic programs. All large systems have this program as a way to access the system if everything else fails. It is the responsibility of management to restrict the use of the program on a strictly as needed basis and to keep access limited to only those who have a valid requirement to use it. Control of the programs is crucial to good system security. Detection is extremely difficult. Because the system can only be accessed using the superzap program, and because a clever programmer can make minute changes to the operating system to their advantage, ascertaining that computer systems are being manipulated is difficult. Comparing master copies and bringing in outside technical help to review operational programs is the best means of determining if a problem exists.

19

### LOGIC BOMBS

Logic bombs are computer instructions which are entered into the systems through a trojan horse technique. Logic bombs have a much more dangerous connotation associated with them. The unauthorized computer instructions can cause an entire computer system to shut down. All it involves is a few lines of program which are set to go off at a preset time and a computer system can be rendered completely useless. Detecting a logic bomb is similar to finding a trojan horse.

-----

Operating systems must be compared (from a copy of the master) and changed periodically to detect any unauthorized routines.  
20

One employee set a logic bomb that would go off if he was ever fired from the company. The result would be to completely erase every customer file from the computer records.  
21

### VIRUSES

One of the newest forms of computer sabotage is the creation of the virus program. A virus program is an unauthorized program which copies itself and gets into the main logic of the computer. It then effects everything that comes into contact with the operating system. The virus can cause phrases to appear on the screen, or they can cause all data files to be destroyed. Any program which subsequently comes into contact with the CPU of the infected computer, will carry the virus code. If this program is used in another computer, then the new computer will be "infected" and will in turn infect other programs. The effect is that the virus is quickly copied and distributed to other systems. Many viruses also come from computer bulletin boards. Downloading the bulletin board message to the computer will cause the virus to be sent with it; infecting the computer in the process.

-----  
20

Ibid. pg 242-243

21

Interview, Price



A graduate student recently devised a computer virus that went along an unclassified network system. Numerous companies and research facilities were connected to the system. Every computer which linked up with the net was infected with the virus. The result was that companies and government agencies were forced to shut their systems down due to a loss of memory and computing power.

The best prevention from computer viruses is to keep computer programs separate. Sharing of disks is the most common cause for the spreading of the virus. Each company computer should have its own system software, and they should not be passed around. Observant employees can also help to slow the duplication of the virus. Noticing that a computer is taking an excessively long time to perform its actions, or realizing that available memory space is being used up, is a good sign that a possible virus program has been used. Managers should immediately shut down the system to prevent further spread. It is also imperative that backup copies be made frequently in the event that a virus destroys the files on a data disk.

22

## CHAPTER 4

### THE PEOPLE INVOLVED

In order to detect computer crime, a manager must have an idea of who is responsible. Computer theft can be committed by almost anyone who has the access and the ability. Donn Parker, senior systems consultant at SRI International, says that three conditions are necessary to enable a would-be criminal to commit computer crime - knowledge, access, and resources. <sup>23</sup> As a result of the increased use and availability of personal computers, computer crime can be carried out thousands of miles away with little chance of detection. Still, a "typical" computer criminal has certain characteristics which can be observed:

(1) They tend to be young. The average age is between 18 and 25. This is possibly due to the fact that the younger employees have had more experience and education with computers. Research has shown that many of the so called "hackers" are high school or college students who have above average intelligence but are underachievers. They tend to be loners who try to gain attention through their computer abilities. They often come from broken families, or families where both parents work and they are left to themselves. They often become obsessed with breaking into the system, giving up their school work, jobs, and even family to achieve their

-----  
23

"Preventing Computer Fraud - A Message for Management,"  
CPA Journal, November 1987, p 36-37.

goal.

(2) Perpetrators also tend to be bright, eager, motivated and adventurous - the same traits which companies are always looking for in employees. The vast majority of computer crime comes from the employees within the company. The range of criminal extends from the lowest level clerk who is responsible for data entry, to the entire division of a company who act together to steal from the computer system.<sup>24</sup>

Reasons for employees being the most common abusers include a feeling that the company "owes" them something. They feel the company has not fully compensated them for their efforts. Because many companies have poor security systems, and even poorer policy procedures, it is very easy for these people to use the computer for their advantage.

One study has shown that employees who are overqualified often try to break the security system to make their jobs more appealing. They are young and bright and feel they can beat the company. They may do this as a way of revenge or they may even feel they will ultimately help the company by showing the weak points of the security system.

(3) Computer criminals are often in a position of trust within the company. Employees who are very familiar with the system, and are allowed to work with it on a continual basis,

may take the opportunity to abuse it. There are numerous positions within the company that have critical access. These include, from lowest risk to greatest: peripheral operator, job setup clerk, tape librarian, data entry operator, computer operator, systems operator, and systems programmer. The greatest possible risk comes from the security specialists whose job it is to design the security system.<sup>25</sup> It often takes more skill, knowledge, or access than one person alone possesses. "Collusion tends to involve a technical person who can perpetrate the act and another person who is in a position to translate the act into some form of gain."<sup>26</sup>

Management procedures are the most important safeguards to a secure system. Thorough screening of employees is the best beginning step. A full background check must be conducted for as many employees as possible who have sensitive access to the system. In addition, employees must be educated in computer security; to be made aware of the effects of an insecure system. Another important management step is to have separate duties so that no one person has total access. It is incumbent upon managers to develop written procedures and policies which are carried out concerning the use of the computer. Managers must be continually on the lookout for radical changes in employee behavior. Uncharacteristic

-----  
25

Parker, Computer Security Management, pg. 153

26

Parker, Crime By Computer, pg. 51

spending habits are a good clue that the system might have been tampered with. Employees who seem to be having personal problems must be observed closely to insure they do not try to commit computer crime. More on management will be said later in this paper.

## CHAPTER 5

### RISK ASSESSMENT

Perhaps the most important aspect of a managers job in preventing computer abuse is to adequately identify the risks which are present inside and outside the corporation, and taking measures to lessen their effect. This risk assessment helps to point out weak areas which need to be addressed. As computers become more advanced, and people begin to utilize their power, it will become increasingly important for managers to be aware of where the risk is coming from. When analyzing the level of risk exposure, a manager must determine (1) assets which are vulnerable to loss, and (2) the sources of potential threat to those assets.<sup>27</sup>

One of the first ways in which a security manager can assess his computer system and the risks involved, is to set up an investigation team. The mission of this team is look at all facets of the company and critically assess their relative risk associated with computer misuse. The key players in the team should be a director of security, an investigator, an information specialist, an auditor or accountant, and a company lawyer.

The director of security should be the overall coordinator of the team. It will be his or her job to collate all the information from each of the other team members and

27

Baker, Computer Security Handbook, pg. 29.

brief the top management on their findings. The investigator is responsible for observing and following up on information discovered by either himself or by the other members. He/she plans surveillance, interviews with suspects and employees, conducts background checks and insures any suspicious activities are checked. The management information specialist is there to provide expert guidance on the workings of the computer system. They assist in translating information and testimony into a language which can be understood by the layman. The accountant or auditor should be knowledgeable on how computers can be used to manipulate files and accounts. They are given the task of searching computer files for symptoms of fraud and deviation from standard operating procedures. Finally, the lawyer is the expert in trial litigation. He/she reviews the investigative process and the evidence gathered to insure that it can be used for trial purposes. They also insure the company does not violate the privacy of the workers.

It is clear from the roles of the team listed that they must be experts in their fields. The investigation must be carried out precisely and thoroughly to ensure that all areas are covered. The first responsibility of the investigation team is to determine the assets which are vulnerable to computer theft. Each company will have different items which are important to them. A bank or other financial institution will put more emphasis on their automatic financial

transactions and accounts, whereas a manufacturing firm will take great care to safeguard their plans and construction models. There is no single list which encompasses what a company should protect. This will be the responsibility of individual managers to determine. Some of the more common computer assets to a company are financial transactions, systems programs, application programs, trade secrets, accounts receivable ledgers, and future plans. Any company which regularly uses a computer in its operations should assess the importance of that data. They must determine what the cost of losing it would be and what it would cost, if they were able, to replace it. This is one of the most important jobs for supervisors and other management to accomplish. One method known as the Delphi technique has proven very successful in identifying crucial information. The Delphi technique is basically a large brainstorming session where affected managers assemble and take turns giving their estimates of the value of their assets. Each manager is given the opportunity to present his views and hear the opinions of others. Each estimate is then revised according to the feedback received from those present. After several iterations of this procedure, a better assessment of the value of the assets is gained. This is important because it will form the basis for incorporating a security system. Obviously



the more valuable the information or asset, the more priority it will receive in securing it.

The next responsibility of the team will be to identify the sources of threat to the company. This should be done by identifying the people who have the skill, knowledge, and access to commit computer fraud. According to Richard Baker, there are four basic sources of loss from people according to their skill level:

- 1) People with physical access who have the capability to perform physical destruction
- 2) People with access who have operational capabilities
- 3) People with access who have programming capabilities
- 4) People with access who have electronic engineering capabilities

A company should have this information by developing job descriptions on employees, looking at personnel files, customer lists, vendor and creditor lists, and especially reviewing the previous experiences of computer loss.

The team should be wary of employees or customers who show a marked interest or dislike regarding the company. An employee who is fired and has had access to the company computer should be monitored to insure he/she does not take their aggression out on the company. A simple management technique would be to have a written and enforced policy of changing passwords any time an employee leaves or is dismissed. He should not be allowed to go back to his work

station without being accompanied by his supervisor. An escort should be present until they are out of the building.

In order to best identify the human sources of threat, the investigation must identify the motives which people might use to attack the company. A list of general motives was developed by psychologists which might explain a persons behavior to commit computer fraud. These motives include a feeling of incompetence, personal problems, desire for personal gain, and extreme advocacy based on economic, political, social, or religious beliefs. Such behavior can be extremely difficult to detect. Managers must be aware of changes in their workers. A worker who starts showing up late or missing work, or who turns in substandard work could be someone who has personal problems. They must also be aware of changes in their economic behavior. If a data processor who earns \$5 an hour starts driving an expensive car, managers must be on guard that their system might have been tapped into illegally. It is the responsibility of each supervisor to continually monitor the habits of their workers. Sudden changes should be noticed and acted on if any suspicious activity is noticed.

A different type of threat which security managers cannot stop, but can take measures to reduce their effect are the forces of nature. Tornadoes, fires, and floods cannot be

prevented, but the damage can be controlled by preparing for the consequences. Fire protection devices can be installed which will immediately dampen the fire without destroying the equipment. Backups of data files and records should be kept a considerable distance from the main computing center. This will provide a means for retrieving data if it is lost. The important thing for managers to consider is to make contingency plans. They must know what to do if Acts of GOD occur. As an old saying goes, "proper planning prevents poor performance."

Management can also undertake additional means of investigation to assess their computer security. One of the best forms of risk evaluation is scenario analysis.

Scenario analysis is designed to put problems into an understandable format for managers. Rather than being completely technical in nature, the scenario analysis will put the information into a problem-statement format. It will point out weak areas in computer security by developing a set of problems which describe a related range of threats based on real occurrences. The scenario procedure would be as follows. For each major threat which is determined by the investigation team, a scenario would be developed which describes how losses from the computer system might occur. These scenarios are then passed to the management of each section of the company who give their opinion as to the credibility of the scenario to happen. They will also give their judgement as to how to

prevent the scenario from actually happening. These scenarios are then used to test the computer security system. Next a group of security specialists should attempt to gain unauthorized access to the system. This could be anything from stealing an unsuspecting employees password, to disguising themselves as bank inspectors and requesting access to the computer. The important thing to notice is that this is done to identify existing weaknesses. The majority of crimes are committed by employees who have unsupervised access. By pointing out the means by which they can commit fraud undetected, managers and supervisors will be able to limit computer misuse.

31

The advantage of the scenario method is that it helps to point out the weak links in the computer system. A company will be able to determine a list of current protection, a list of planned protection in which managers indicate what they are doing for the future, and a list of remaining problems which cannot be addressed at the present time. Another, more subdued advantage, is that it forces all managers to work together to resolve deficiencies. It provides a stronger communication system for the future.

## CHAPTER 6

### SECURITY MEASURES

The need for adequate protection of computers and their resources will continue to increase. The responsibility of designing the security system will normally fall to the company's security manager.

The first obstacle for the security manager to deal with will be to find the type of security system which is compatible with the company's computers. There are two options available. The first is to buy a product already on the market. There are numerous programs designed to provide protection of software and data files. These programs have security measures such as password protection, audit trails access control, transaction logging, and some even report to be able to protect against computer viruses. Security programs such as these help provide management the ability to better detect computer fraud.

The advantage of off-the-shelf programs are their lower cost than custom made programs, and their ready availability. The disadvantage of these types of security systems is that they may not fully meet all the needs of the company. Training programs will be sparse, and if not installed correctly, the system might prevent authorized users from gaining access when they need it.

The second option is for a security system to be

developed specifically for the computer system of the company. The obvious drawback to custom made programs is the high cost required for specialists to design the system. The advantage is that the system will perform the procedures which management requires. It will also have better support from the developer in areas such as training employees. The company will have a direct point of contact to get hold of in the event problems occur.

The needs of the company will dictate whether a market program is used or one is specifically made. Either way, a useful security system must provide three lines of defense against computer fraud: (1) prevention, (2) detection, and (3) limitation.  
32

Prevention restricts the access of potential criminals to the computer facility, terminals and data records. Detection sets off a report that someone has gained unauthorized access. Limitation will help to reduce losses in the event the security system is bypassed. An in-depth look at each area will show the technological controls which will ensure a secure computer system. The management chapter will deal with the administrative controls that supervisors can implement.

### PREVENTION

Prevention is the front-line defense to restricting  
-----

unauthorized access and use of the system. The increase in technological advancements have made access protection much more sophisticated. Tamper-proof terminals, secure interfaces, protected cable routes, encryption of data, and call back techniques have been improved as a means of controlling entry. The ultimate objective of a prevention system is to ensure that only legitimate users are allowed entry. Proper prevention of unauthorized use requires two forms of control: (1) entry, and (2) access-control. <sup>33</sup>

#### ENTRY

The most reliable means for denying access to unauthorized people is to set up an entry control procedure. Entry control refers to established procedures and technical barriers which help to keep sensitive computer areas secure.

The first control is to have procedures which are enforced. The most important safeguard for securing an area is not to draw attention to it. The computer center should be indiscreet, looking as if it were any other part of the building. There should be no signs which point out its existence. Employees should be instructed not to refer to a particular area as "the computer area." Inside the center, security guards should be posted. Employees should be issued

badges which inform the guards as to their level of access and whether they are allowed entry. If a lock is used, keys should be given only on a limited basis and these people should be held directly responsible for their proper use. Employees must also be trained to question and challenge anyone who is not permitted access who attempts to enter. These procedural controls are the responsibility of management to develop. They must be trained and enforced in order to keep the computer secure.

The second means of controlling entry is through technological barriers. New and advanced methods have been developed which can permit entry only to those people matching a specified characteristic. These processes are called biometric parameters. A biometric characteristic is one which is unique to one individual. For example, special locks have been constructed which will permit opening only if a users fingerprints match the prints in the computer's file. A person would put his hand on a scanning device which compares his fingerprints with those on file. If they match the person is granted entry. Biometric locks can also be constructed to compare the retina pattern of the eyes, height and weight distribution, and even signature style. There are some drawbacks to these systems. The first is the cost. Biometric locks are very expensive to install. Large data bases must be created and the scanning equipment must be very sensitive in measuring the personal characteristics. The



locks may also be too sensitive. If a person should cut his finger, the pattern of the fingerprints may be different enough that the scanner will not permit entry.<sup>34</sup>

Other barriers to entry include closed circuit television, remote locks, double doors, and turnstiles with electronic locks. These systems have proven very effective in thwarting would-be criminals. The important consideration for the security manager is the cost-benefit analysis. Installing any electronic security measures will require a good deal of money. Each of the different functional managers must determine the value of the information in the computer system and decide if the cost of the security system is worth the outlay. Good communication between the different sections of the company and honest appraisals of their informational assets is the only way to justify the cost of the security.

#### ACCESS-CONTROL

An access-control system has certain specifications which must be met. It must first determine the authorization and identity of users. It must also be able to determine the level of access the person is permitted. Programs must have a range-level of accessibility which can only be executed by authorized people. The following security measures are intended to provide prevention and control of data.

-----

## PASSWORDS

Passwords are the simplest and most used form of initial protection. They are designed to permit only those people with proper credentials to use the computer. The password is a unique identifier which an individual enters into the computer before any programs or data can be accessed. The password system has some major drawbacks if not used correctly. The first is the ease of theft. If the user is not taking precautions to restrict viewing while entering, anyone will be able to see the password and will thereby have a way of entering the system. Another problem is that many passwords are chosen which the user can easily remember. Passwords such as a child's name or social security number can be easily obtained and later used by possible perpetrators. There are certain password protection objectives which are crucial to proper management:

- (1) Reduce the possibility of guessing by trial and error
- (2) Reduce security exposure by requiring passwords to change at random intervals
- (3) Prevent the person responsible for allocating ID numbers from knowing the users password

Security experts further recommend the generation of passwords having the following requirements:

- (1) Selection and assignment - A password should have at least six randomly generated alphanumeric characters. Users should be given these passwords rather than devising their own to keep the passwords as random as possible.

-----

(2) Frequency of change - The system should be designed to automatically change the password at random intervals.

(3) Repeatability - The password attempted should be maintained on a list and a set number of attempts should can only be made. Any attempts after the predetermined number, should result in confiscation of the password and prohibit any further attempts at logging-on.

(4) Encryption - All passwords should be entered in a one way encrypted form. That is, while the password is being entered, no one should be able to view the characters.<sup>36</sup>

#### ACCESS-RANGE

The second part of the security system is to ensure that users are allowed access only to what they are authorized. Most large companies have levels of clearance for access. For example, an accounts payable clerk would have access to the accounts payable ledger, but could not view the personnel records. The head of the division would have access to all information pertaining to the division, but may be denied entry to the entire financial records of the company. The level of access granted to an employee is a matter of policy. The important role of the access-control system is to keep unauthorized people from viewing data they are not cleared for.

The computer system is designed to identify the user through the ID number and the password, and only grant access to the level they are permitted. A list of user IDs is

prepared which state the range of access for each employee and is programmed into the computer. If the user attempts to enter the system beyond their authorized level, a warning is first issued informing them that they are not allowed the requested information. If the user attempts to download the information again, the system can log them off or even confiscate their ID and prohibit further use.

The advantage of the access-levels is that it will keep users from prying into unauthorized information. It can also narrow down the people responsible if computer fraud is committed.

### DETECTION

Detection is designed to locate unauthorized users who have bypassed the prevention safeguards. If detected quick enough, any damage to the computer files can be minimized. The most useful means for detection is through properly administered audit trails.

### AUDIT TRAILS

An audit trail is a means of identifying the people who have used the computer system during a given period. It is internally produced during the computer processing. A thorough system will maintain a series of different logs:

- (1) All unsuccessful sign-on attempts and unsuccessful attempts at accessing unauthorized levels must be logged. The user ID, attempted password, and range level requested must be noted to allow for evaluation of possible security violations.

(2) User IDs which are not used for a certain number of days should be flagged. Reasons for their lack of use should be identified (vacation, sickness etc.). Any attempts to use these IDs should be noted. It will help to ensure that no one is trying to get into the system through a password that belongs to someone who is known to be absent. It also ensures that employees who leave the company, or no longer have a "need-to-know" do not ultimately attempt to use the computer when not allowed.

Detection is a valuable means of combating losses from computer crime. If action is taken as soon as it is discovered that an illegal person is in the system, the chances for catastrophic losses are reduced. Management must be on guard for any signs of tampering or fraud. Original records should be gathered and reviewed and tested against the current record to see if any alterations have occurred. As always, the task for timely detection and reaction falls on the manager. They must not become lax in investigating possible security breaches.

#### LIMITATION

Limitation could be considered a synonym for good contingency planning. The company must make arrangements to recover from the effects of would-be perpetrators.

Recovery must be available for a wide range of events. Hardware failure, software bugs, operator and data errors must be expected and accounted for. Systems must be designed which periodically update their files into the main memory.

These forms of loss are not generally from computer misuse. They are part of the every day errors which come from people and the effects of computer systems malfunctioning. The security specialist is more interested in recovery from large scale disasters and losses from computer criminals.

Good planning will help to limit damage. Placing back-up files in the same building as the computer system is inviting trouble. They should be located as many miles away as is economically feasible. A plan must be set up which will allow rapid replacement of lost files and programs.

Computers should be programmed to deny transfer of funds over a certain level. By flagging these events, and making an immediate investigation, losses can be stopped. Security must have full support from each employee. Techniques for proper managerial control of employees and computers are a necessity.

## CHAPTER 7

### MANAGEMENT'S RESPONSIBILITIES

Any computer security system is only as good as the people who control it. Without proper procedures and safeguards, the most elaborate system will be useless. As has been noted before, the vast majority of computer crime is committed by employees who have the skill, knowledge, and access. The American Bar Association ranked the following as requirements to prevent and detect computer crime:

- More comprehensive and effective self-protection by private business
- More education of users concerning vulnerability of computer usage
- More severe penalties for fraud perpetrators
- Greater education of the public on computer crime<sup>38</sup>

Many companies feel that a system which is too restrictive will inhibit the ability of their employees to work freely. The reason that for a company to succeed, security must take a back seat to accelerated design and production schedules. They rely instead on the integrity of their employees. Sensitive work is allowed to be removed and taken home in the interest of meeting tight deadlines. Subsequently, the security practices of many companies are loosely practiced. Today's computers contain an enormous amount of information. Many computers have been broken into by "hackers" who bypassed simple security barriers. These

---

38

Paroby, "Preventing Computer Fraud," pg. 36.

computers contain billions of dollars in financial assets, highly secret military records, important research data, and a host of other sensitive information. How can management reverse this trend? How do they implement procedural controls which provide adequate security to their computer files?

Effective laws regarding computer crime are still in their infancy. The ones which are in use do require business to take certain actions if they hope to prosecute would-be criminals. The Foreign Corrupt Practices Act of 1977 requires that publicly held companies "devise and maintain a system of internal accounting controls sufficient to provide reasonable assurance that:

Transactions are executed in accordance with management's general or specific authorization.

Transactions are recorded as necessary to permit preparation of financial statements in conformity with GAAP or any other criteria applicable to such statements, and to also maintain accountability for assets.

Access is permitted only in accordance with management's general or specific authorization

The recorded accountability for assets is compared with the existing assets at reasonable intervals and appropriate action is taken with respect to any differences." <sup>39</sup>

Complying with the laws requires careful planning and work by the organization. The first step for management to take is to (1) design an internal control system that



minimizes risk of loss from errors and irregularities, (2) maintain confidentiality of information, and (3) insure continuity of operations.<sup>40</sup>

There are two main objectives for instituting an internal control system. The first is to insure that development of and changes to programs are authorized, tested, and approved prior to being placed into use. The second is to keep access to data files restricted to only authorized users.

When a new program is designed or purchased, it should not be used until it has been authorized and tested. Written procedures must be developed which prohibit any program from being used without prior consent of the supervisor. Random checks of the computer system for unauthorized programs should be conducted. Periodic comparisons of master programs with programs in the system should also be done to insure that no illegal commands have been entered.

Data file access controls help to ensure the integrity of the company's data. Controls should "provide reasonable assurance that the correct files are used in an application, data files are restricted to authorized users, and data is not changed without proper authorization."<sup>41</sup> Passwords and entry procedures based on personal characteristics have proven very beneficial in keeping unwanted persons out.

-----  
40

Ibid., pg. 38.

41

Ibid., pg. 40.

Companies are beginning to feel the effect of employee fraud and theft. The most important consideration for successful managerial control is to have the full cooperation and assistance from all employees. Companies have begun to hire consultants who specialize in the training of workers on safe computing practices. Mandatory security classes are conducted which stress the need for proper procedures to be followed. Areas such as confidentiality of passwords, refusing requests for information from unknown or unauthorized persons, challenging of employees who conduct themselves improperly, and reporting of any suspicious activity are stressed in the classes. Employees are reminded of the importance of their work and the consequences of having it stolen. Some companies have even started to reward employees who catch a person attempting illegal access.

Businesses have also started to schedule ethics courses. These programs are administered to every employee from the President of the company down to the newest data clerk. Their purpose is to remind everyone that they are responsible for the highest levels of integrity. New employees are often required to sign a non-disclosure statement which prohibits them from administering any information to another company. Failure to follow the non-disclosure agreement could lead to

42

criminal charges.

There are several requirements which managers alone are required to implement. Controls such as forced vacations, random checks of records, and segregation of duties should be used as a way of detecting possible fraudulent activities. Separation of duties refers to having different people responsible for record keeping, physical custody of assets, and general supervision and authorization of transactions. The objective is to have split control over certain aspects of the company to keep one person from having the opportunity to gain improper access.

Effective management is much more than just writing policies and regulations. Managers must make every effort to work with the people who use the computer. Training must be done so that each worker is familiar with the security system. Supervisors must take a personal interest in their people. Counselling sessions are an excellent method for reducing the possibility of an angry employee taking their frustrations out on the company. Trained psychologists must be made available to help workers with personal problems. Maintaining a high morale is essential to reducing the theft due to employees.

The responsibility and accountability of managers and supervisors cannot be overstated. Maintaining a constant vigil on the day-to-day operations is vital in keeping computer assets secure. The highest level support must be given. The fear or mistrust of computer security systems must

be overcome to make security effective. The Justice Department has conducted a study on the effect of computer crime and has developed a set of guidelines for better control:

- Store passwords in code within the computer
- Prepare a signed agreement that details the user's rights and responsibilities
- Bill all computer use to the user's department. This gives the department manager a chance to check for unauthorized use
- Maintain logs and documentation of all program changes
- Restrict access to utilities that could bypass security
- Control access to system documentation
- Keep detailed records of access to sensitive files
- Establish special passwords which are modified frequently for critical data
- Automatically disconnect unneeded access lines during off hours
- Determine normal use patterns for authorized users.
- Note and check any significant changes<sup>43</sup>

Managers must strive to set their security goal in conjunction with these guidelines.

CHAPTER 8  
LAW AND COMPUTER CRIME

Before computers, the average bank robbery was about \$10,000. The average computer robbery is between \$100,000 and \$500,000. Even more alarming is the fact that 82% of members of the Data Processing Management Association knew of incidents of computer crime, only 6% knew of cases where a person was prosecuted, of these six, only 1 in 20,000 go to jail.<sup>44</sup>

The reasons for such poor percentages of conviction stems from the lack of workable computer crime laws, both federal and state. Forty Seven states have thus far enacted some form of legislation. The laws are too narrow in scope however, and do not resolve the problems of evidence or jurisdiction. Prosecutors are finding the existing laws make only specific acts illegal. The intent of the majority of laws is directed only at the theft of money. Any other act committed by computer is not prosecuted under computer crime statutes.<sup>45</sup>

Four types of computer crime have been identified in existing legislation. (1) Introduction of fraudulent records or data, (2) Unauthorized use of computer facilities, (3) alteration or destruction of information, and (4) theft of

<sup>44</sup> Jay Nawrocki, "There are too many loopholes; current computer crime laws require clearer definition," Data Management, July 1987. pg. 14.

<sup>45</sup> Ibid., pg. 14.

money by electronic means.

While these areas may seem to be broad enough to cover the majority of computer related crimes, courts have required that property be visibly damaged or removed before convicting an individual for unauthorized use. The problem is that computer resources and information can be used without damage or removal of personal property. There is no tangible evidence to indicate the unauthorized use of the computer information. The courts have held that only the electronic pulses would give concrete proof of illegal use. If there is no record of the pulses then there is no tangible evidence.<sup>47</sup>

Another important consideration according to the courts is the question of jurisdiction. Courts have historically convicted criminals only if the crimes were committed in the jurisdiction in which the legislation was enacted. It can be difficult to determine where the crime actually took place. If the crime was committed by a computer in another area, will the people be subject to laws in the area where the crime was enacted, or where the computer facilities reside?

The third area which makes computer crime difficult to effectively legislate is the question of privacy. To what extent are managers permitted to conduct background checks on

-----  
46

Ibid., pg. 15.

47

Ibid., pg. 15

their employees? To what degree may personal files be maintained on a company computer? These questions are being asked in the courts. Companies which use computers to perform checks on their employees are quickly coming under scrutiny from the courts as a possible invasion of privacy. Without the ability to check on workers, companies may find it difficult to monitor their work performance. It will also be difficult to notice a major change in their spending habits which could come from stealing of company resources. These questions are being debated and will not likely be quickly answered in the near future.

Many if not most prosecutors are computer illiterate. The same goes for the judges. They usually have no expertise in operating computers. They must often rely on the word of co-workers or even friends on working the computer. This lack of knowledge makes it difficult to successfully prosecute an intelligent criminal who can hide his work using the computer.

There is some promise for new federal legislation. President Reagan signed two bills which make it a felony to electronically break into, steal, or alter computer data. These acts, the Electronic Computer Privacy Act, and the Computer Fraud and Abuse Act, would make it a federal crime to gain unauthorized access to data in any financial institution computer, federal computer, or any interstate computer. Trespasses of more than \$1000 in software damage, or actual

goods, or services are considered felonies and are punishable up to 5 years in jail. The catch to the law, however, is that if stolen data is not linked to a loss of goods and services greater than \$1000, it is considered a misdemeanor, not a felony.<sup>48</sup>

The important area for managers to be concerned with in the new law is the requirement of actions of the offenders to be documented. This places the burden of proof on the owners of the data. In order to document actions, managers must maintain complete audit trails of all data accesses - both authorized and unauthorized. If there is no audit trail, the courts will not act.

Audit trails consist of keeping track of who uses the computer and for what purpose. Audit trails can come from off-the-shelf software or can be custom programmed for a company's computer. They must keep track of who is accessing the computer and the files which were requested.

Computer legislation is still narrow in scope and difficult to employ. The Data Processing Management Association has worked with federal and state authorities to devise legislation which would be effective. They have developed a set of guidelines for a Model Computer Crime Act, these include:

-----



unauthorized use or access of computer resources  
unauthorized release of computer information  
unauthorized copying of software  
unauthorized modification of computer resources  
unauthorized destruction of computer information  
unauthorized denial of access to computer resources  
(ie implementing a program which would deny access  
to authorized company employees) 49

These guidelines are a start for usable laws to be enacted to combat computer abuse. It will take a combined effort of federal and state agencies to make these laws work.

## SUMMARY AND RECOMMENDATIONS

The widespread increase of computer crime and the economic impact caused by computer fraud has created the need for proper security of company computer systems. The managerial considerations involved in safeguarding assets, information, trade secrets and financial information are becoming extremely important. As computers are used for more and more purposes, the chances for their misuse becomes greater. The purpose of this study has been to acquaint the reader with an overview of the various methods of computer crime and provide some examples of the available means for combating it.

When examining the need for a security system, a company must fully evaluate their business; both now and for the future. A realistic assessment of the assets controlled by the computer must be undertaken. This assessment must then be used to provide a cost/benefit analysis to justify the expense of the security system. Providing adequate security at acceptable costs is an important issue for the senior staff of the firm to decide.

A useful security system must be designed to expand as the needs and uses of the company grow. Off-the-shelf security systems may or may not provide this flexibility. Their main benefit is the lower cost. The company must decide whether this lower cost will outweigh a more expensive system which is customized to the companies computer. Managers

must also assess their ability to train employees inhouse. Does the market program adequately prepare workers to use it, or would the company have to hire an outside consultant to train the operators? There are other considerations to deal with. For example, does the vendor provide troubleshooting services? Will they upgrade the system at a reduced cost as new features are added? Will they provide maintenance to include adequate documentation? These are all questions which a company must answer prior to purchasing a system.

The ultimate defense against computer fraud comes from the honesty and integrity of the workers in a firm. A company which takes the effort to keep a high morale will be less likely to face an angered employee who takes his frustrations out on the company. Providing for the needs of the workers will help to keep their minds on the job and not on personal problems. Managers must be on the watch for changes in attitudes and work habits. Quick action will help to alleviate problems and may prevent losses.

There are numerous checklists which can be obtained which are designed to help a company secure their computer. While these can be useful, the most important assets available are common sense and good managerial control over the system. Safeguards such as password protection and range limitations can be easily implemented to reduce losses. Close adherence to policies regarding computer use can assist managers in keeping unauthorized users from gaining access.

The burden for securing a computer system falls squarely on the managers and supervisors in the company. They must be aware of as many new forms of computer abuse as they can. This requires that they stay current in the methods and prevention of computer crime. Failure to do so may cause them to be the victim of computer theft.

As companies continue to become more dependent on the services of computers, the need for safety increases. The value of this study has been to orient computer users on what they can and must do to keep their computer assets from being lost or stolen. They owe it to the business and the stockholders to prevent computer crime.

## BIBLIOGRAPHY

### Books

- Baker, Richard H. The Computer Security Handbook. Blue Ridge Summit, NJ., Tab Books Inc., 1985.
- Francis, Dorothy B. Computer Crime. New York, E.P. Dutton, 1987.
- Norman, Adrian R.D. Computer Insecurity New York, Chapman and Hall, 1983
- Parker, Donn B. Computer Security Management. Reston Virginia, Reston Publishing Company, Inc., 1981,
- Parker, Donn B. Crime By Computer. New York, Charles Scribner's Sons, 1976
- Parker, Donn B. Fighting Computer Crime. New York, Charles Scribner's Sons, 1983.
- Schuller, Randall S. Personnel and Human Resource Management. St Paul, MN., West Publishing Co, 1984.

### Periodicals

- "Computer Crime Hits Hard." OECD Observer, April 1984, pg. 36-39.
- "Computer Fraud." Management Today. 2 Sep 1983. p. 24.
- Gullo, Karen. "Security is Loosely Practiced at Young Super Computer Firms." Datamation, 1 Jan 1988, p 26.
- Marsh, Gerald V. "The Practitioner and the Computer." The CPA Journal, 15 October 1988. p 107
- Nawrocki, Jay. "Too many loopholes." Data Management, July 1987, p 14.
- Paroby, Martin J. "Preventing Computer Fraud - A Message for Management." The CPA Journal. November 1987, pg 36-45.
- "Programmed to sneeze." The Economist, 28 November 1987, p 90.
- Rhodes, Wayne L. "Securing the IS Jewels." InfoSystems, April 1987, p 8.
- Srinivasan, Cadambi A. and Dasher, Paul E. "Access Control Assures Network Security." The Internal Auditor, Aug 1986 pg. 37-43
- Thomas, Michael D. "Rise in Computer Oriented Crimes." National Underwriter, 1 August 1984, p. 35.