University of North Dakota

UND Scholarly Commons

Theses and Dissertations

Theses, Dissertations, and Senior Projects

11-1983

Protecting The Medium-Sized Buisness Computer

Michael J. Doonan

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

Part of the Business Commons

Recommended Citation

Doonan, Michael J., "Protecting The Medium-Sized Buisness Computer" (1983). *Theses and Dissertations*. 4449.
https://commons.und.edu/theses/4449

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.commons@library.und.edu.

PROTECTING THE MEDIUM-SIZED BUSINESS COMPUTER

BY

Michael J. Doonan

B.S. in Aeronautical Administration,

Parks College of St. Louis University, 1978

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 Business Administration

The University of North Dakota Graduate Center
November
1983

This independent study submitted by Michael J. Doonan 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.

Paul Nowak

Faculty Advisor

PERMISSION

Title: Protecting the Medium-Sized Business Computer

Department: School of Business and Public Administration

Degree: Master of Business Administration

In presenting this independent study in partial fulfillment of the requirements for a graduate degree from the University of North Dakota, I agree that the Library of this University shall make it freely available for inspection. I further agree that permission for extensive copying for scholarly purposes may be granted by the professor who supervised my work or, in his absence, by the Chairman of the Department. It is understood that any copying or publication or other use of this independent study or part thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to the University of North Dakota in any scholarly use which may be made of any material in my independent study.

Michael J Doonan
Signature

22 November 1983
Date

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

ACKNOWLEDGEMENTS

The author is very grateful to Dr. Paul Nowak, Advisor, for his constructive critique and for providing an insight to the administration of the Graduate School at Minot AFB. Appreciation and thanks are also extended to Mrs. Jean Parish, who insured all of my required paperwork was completed, and to Ms. Sue Branson, who typed this study.

Finally, the author wishes to extend a personal thanks to the staff of the Graduate School, especially Dr. Robert Bertsch, Dr. Adnan E. Daghestani and Dr. Orville Goulet for their instruction, guidance, and advice.

ABSTRACT

Protecting the Medium-Sized Business Computer

Michael John Doonan, B.S.

The University of North Dakota Graduate Center, 1983

Faculty Advisor: Dr. Paul J. Nowak

Computers were first introduced into our lives in 1944, when the first one was designed and built for the Army. They were able to process simple information faster than man, allowing him to concentrate on more difficult problems. Progress came quickly and the first commercial use of the computer was in 1954.

Today, computers are recognized as having a tremendous influence on our daily lives. They have been successfully incorporated into almost every aspect of human endeavor.

Computer crime is an unfortunate reality in today's world. If the crime is detected at all, the loss may very well run into the millions of dollars. There are countless threats of penetration to a computer system. The data-processing manager must do his best, within company constraints, to combat these different threats. These threats come from a variety of sources. The internal threats can range from embezzlement, fraud, blackmail or program substitution/contamination. External threats can take the form of direct sabotage, wiretapping, program modification or natural disaster.

A variety of different protective techniques and devices can be implemented to guard against system penetration. It

is up to the manager to decide what is the best alternative to suit his needs. Guarded entrances, sign-in/sign-out logs and separation of duties could be an effective protection against internal tampering. If these fail, the manager would have to employ more stringent controls over computer access. Strict password control could help discourage outsider penetration. Encryption/decryption devices will however, become a strong deterrence to outsider penetration in the near future.

Should a crime be committed against the computer system, there is little legal resource available. Current laws are inadequate as written and need to be updated and strengthened if the penalty is ever going to match the crime.

The information contained in this study consists of a variety of secondary sources. These include current periodicals, library textbooks, newspapers and journals.

No computer system can be totally secure from penetration but with tight controls, the chance of hostile penetration is greatly reduced to an acceptable level. Security is everyone's business when working with the system. Management and employees must become involved if the security procedures are going to be effective.

CHAPTER I

Introduction

Several years ago, computer crime was considered to be the crime of the future. The future has now arrived, and the managers of computerized businesses are faced with extraordinary challenges in preventing abuse of their computer systems. Management must recognize that the threat exists and implement effective measures to reduce the risk of system penetration.

In Chapter 1, we will examine the reason for the study, define several terms which will be used throughout the study, define the problem itself and its subsequent justification, then examine the scope and limitations of the study.

Reason for the Study

This study is being conducted to assist the data-processing manager in identifying possible threats and making the decisions necessary to insure the company's information processing system is as secure as possible.

To make a rationale decision, the manager must be aware of a threat before it can be countered. An effective security system will help prevent the unauthorized use of the company's medium-sized computer.

Definition of Terminology

Access Control

This involves physical barriers such as locks on computer room doors, tape and disk libraries, terminals, consoles and printers. It also means system barriers built into programming and manual procedures which will release a transaction, data or a document only on proper authorization. The difficulty in penetrating a computer system can be increased by having properly structured data bases and an access control program requiring a password, identification and authorization before allowing usage.

System Integrity

A program, device or computer system has integrity when no other paths or processes are available to the user except those explicitly provided by the designers. This stringent control is obviously necessary to avoid deliberate backdoor entry of accidental side effects in the process. In a complex computer system with many interconnections and with programming systems handling simultaneous and unrelated problems, establishing the appropriate levels of integrity is absolutely essential.

Data Base Administration

This involves considerable detail such as maintaining passwords for each data element and insuring that all users understand the size, meaning and characteristics of the data elements. This is not merely a clerical function, nor is it a function restricted to system organization. Owners, users and auditors must participate in the data base administration process. How your data base is managed is a key to your entire information flow.

Computer Crime

A crime which involves either the modification, destruction, restriction, unauthorized reproduction of data or the physical destruction of either software or hardware components. Data can be modified in some way, destroyed by erasing, files reproduced or restricted to certain individuals to render the information unusable to a company. Physical destruction could occur through sabotage, fire, water damage or natural disaster. Another crime involves theft of services which is the unauthorized usage of computer time for personal gain.

Statement of the Problem

Crime by computer affects all of us, either directly or indirectly. The dollar loss is counted in the millions each year as a result of fraud, embezzlement, theft and destruction. The actual dollar amount is impossible to calculate however since many crimes go unreported. Hardware, as well as software components are not safe from intruders, who may range from company employees to terrorists.

The data-processing manager not only has to protect his computer system from hostile intruders, but also against the forces of nature. If the possibility of natural disasters are not taken into consideration, the consequences from one occurring could render a computer system completely useless.

Justification of the Problem

The earliest federal prosecution of a computer crime came in 1966 and involved a young programmer in a Minneapolis bank who instructed the computer to ignore all overdrafts to his account.[1]

Since then, computer crime has been on the rise. Millions of dollars are reported stolen each year with many millions more never reported at all. Unless effective measures are undertaken immediately by the data-processing managers, this type of theft could reach epidemic proportions in the near future. This study helps identify known areas of subversion and recommends various responses to counter these threats.

Scope

This study was written to investigate the various threats of computer crime on commercial medium-sized business computers and was not intended to address the effects on government institutions or military installations. A study concentrating on one of these two other areas would be appropriate for another student.

Several examples of computer theft have, and will be given throughout this study. These have been used to highlight the large sums of money involved in the theft and not as a detailed study of the theft or its legal ramifications. A

[1] Tom Alexander, "Waiting for the Great Computer Rip-Off," Fortune (July 1974): pg 144.

study examining each major reported theft and the social, legal consequences incurred would be a possible topic for a future study.

Within the past year, information on actual computer crimes have just started to become public knowledge. A similar study two years from now will have a larger volume of information available and be able to go into greater detail. There currently is not enough published information to thoroughly examine a specific crime, looking at it only in general terms.

Limitations of the Study

The information contained in this report is based on the results of previously published works. Several attempts at arranging personal interviews with federal and local authorities concerning computer crime were unsuccessful. Only one system in this study is presented, the Univac 1110, and only in a limited way.

This study assumes that the data-processing manager has complete control over the security of the computer facility. This however is seldom true, especially in large companies where politics tend to influence the decision-making process. In addition, the employee's resistance to change is not taken into consideration when new methods to prevent computer crime are implemented.

Methodology

In conducting this study, two steps must be carried out: gathering of information and analysis of information obtained.

This information will be gathered from the available supply of articles written on this subject and these secondary sources will be utilized. These sources include current periodical literature, library textbooks, newspapers and journals.

Summary of Chapter 1

Computer crime is no longer a crime of the future, it is the crime of today which can take various forms. In Chapter 1, the problem and its justification were presented. In addition, the scope, limitations and methodology of the study were examined. In Chapter 2, we will review the available literature concentrating on the threats to the computer system. Also, several different companies and the methods that they employ to prevent computer crime will be presented. The success and failure of these methods will be examined.

CHAPTER II

Literature Survey

In 1944, the first successful general-purpose digital computer, the Mark I was built. It was primarily designed to calculate artillery firing tables. Punched cards fed data into the Mark I, where calculations were made with the use of gears, counter wheels, and other mechanical devices. The results of these calculations were then punched onto a new set of cards for the operator to use.

In 1946, the first truly electronic digital computer, the Electronic Numerical Integrator Computer (ENIAC) was developed at the University of Pennsylvania. ENIAC was able to process information without the use of moving parts. Instead of gears, the ENIAC contained 70,000 resistors, 18,000 vacuum tubes, 10,000 capacitors and 6,000 switches.[2] ENIAC, weighing 30 tons, occupied an enormous room and consumed over 100 kilowatts of power.

Since then, we have progressed through four different generations of computers, each being more advanced than the other. Today, a hand-held calculator can far exceed the computational capability of ENIAC and requires only a few small internal batteries for power.[3] In today's fast

[2] "Big Dimwits and Little Geniuses," Time (January 3, 1983): pg 30.

[3] Herman Lukoff, "From Dits to Bits: A Personal History of the Electronic Computer," (Robotics Press, 1979): pg xi.

paced world, computers provide us with rapid flow of processed information. Computers serve that function well by being able to store, sort and retrieve large amounts of information, in addition to making thousands of calculations. They can be programmed to process tasks in seconds, that would take a man years to complete. Computers have been successfully incorporated into almost every aspect of our daily lives. They design our aircraft, control our traffic lights, monitor our heartbeats and in some instances even select our mates. They compose music and have permitted man to explore his solar system. Recently, Time magazine recognized the computer as having made the single greatest impact on our society for 1982, by naming it "Machine of the Year."

Perhaps the biggest influence of all the computer has made has been in the business community. The first computer acquired for data processing and record keeping by a business organization was installed in 1954 at General Electric's Applicance Park in Louisville, Kentucky.[4] Since then, most businesses now apply some form of data processing in the majority of their day-to-day operations. These include: payroll processing, order entry, inventory, accounts payable, and accounts receivable, keeping track of records, the printing of

[4] Donald H. Sanders, "Computers in Society," (McGraw Hill, Inc., 1977): pg 27.

previously typed text, and a host of other applications that do not require large computations.[5] In carrying out these functions, data processing systems are built around modern electronic computers operating at speeds measured in billioths of a second. They have demonstrated their unique capability to process volumes of data and to transform that data into meaningful information essential in operating a successful business in today's complex society.

Information processing has become a critical support system for today's businessman. At each level of decision making, the manager depends on his data processing systems and wants to be assured of their reliability. He must have confidence, based on continuing control, that the system is doing what is expected of it. No other alternative is really acceptable.

"Crime by computer contributes more and more to the annual costs of crimes against businesses. Because the technology is itself so very sophisticated, management faces a difficult problem in trying to prevent the crime. Moreover, a computer crime is subtle, invisible and not subject to conventional auditing."[6] Computer crime is being looked upon by society as a victimless crime, even in some cases as a gentlemen's crime. All age groups are

[5] Myles E. Walsh, "Understanding Computers: What Managers and Users Need to Know," (John Wiley & Sons, Inc., 1981): pg 1.

[6] "Crime in Service Industries," U.S. Department of Commerce (September 1977): pg 117.

becoming involved in this crime, especially the young who have a tendency to view tapping into a computer system as a challenge - even a type of game. It is essential that management exert additional efforts to both understand the computer and prevent criminal abuse of it.

Abuse however, does occur and in some instances, on a grand scale. "The Wells Fargo Bank discovered a year ago that an employee had used its computers to embezzle $21.3 million, the largest electronic bank fraud on record."[7] The magnitude of the loss itself is hard to comprehend, and this is just one case of reported theft. "The U.S. Chamber of Commerce puts the annual loss from electronic theft at $100 million."[8]

Accurate statistics on actual computer crimes are at best, difficult to obtain and evaluate. This is further illustrated by another article which states, "Embezzlement of funds may be the most frequent form of such crimes, but there are many others, including theft, copying or destruction of important data; invasion of privacy; and "theft of services" (such as an employee using the company's computer resources for his own small business on the side). Estimates of yearly losses range from $300 million to $5 billion."[9]

[7] "Crackdown on Computer Capers," Time (February 8, 1982): pg 60.

[8] Ibid.

[9] Gina Kolata, "When Criminals Turn to Computers, is Anything Safe?," Smithsonian (August 1982): pg 117.

This obvious discrepancy in losses between the two 1982 examples, clearly shows the difficulty in trying to accurately estimate the real dollar cost of computer crime on society.

One reason accurate data is so hard to obtain is that so little of it is ever reported to the authorities. Small companies usually do not have the financial resources or technical expertise to constantly monitor all aspects of their operation. These types of businesses are more susceptible to crimes committed "in-house" by trusted employees rather than from sources outside the company. Such crimes are often not even detected until several months after the employee has left the company, if at all and it is usually too late to recover the loss. A crime like this could literally backrupt a small company. Should a loss occur, the company would be hesitant to admit this loss to the public and their stockholders. William A. Bayse, the Assistant Director for Technical Services of the FBI, points out:

> "There is a lot of reluctance to report crimes because the resulting bad publicity may cost a company more than the loss itself."[10]

If the money could not be recovered, a company might choose to write the loss off and refrain from pressing charges in order to learn how the crime was carried out, so that it is not repeated.

[10] Ibid.

Safeguards must be employed by a company to protect its information processing operations, but at what cost? Economic considerations must always be taken into account. Every successful manager learns to accomplish the job within the established budget, for financial resources are limited. Decisions must be made by the manager to incorporate the most cost effective method available to protect against computer crime.

Computer security was a minor concern in the early 1970's, today however, it is one of the most important responsibilities facing a data-processing manager. "An estimated $200 million was spent for safeguards last year, and the market is expected to grow by $100 million this year."[11] Because of the requirement to comply with the Privacy Act of 1974, security has become even more important by today's standards. The purpose of this study is to determine whether or not a data-processing manager can successfully protect the company's computer system.

Computer crime has struck at not only the small companies but also the major corporations. Losses are counted in the millions, with only a fraction of the crimes ever reported. Human error, which also contributes to this crime can not be completely eliminated.

[11] "Crackdown on Computer Capers," Time (February 8, 1982): pg 60.

Small personal computers pose an additional threat to the system. Worldwide sales of home computers grew from 300,000 units in 1980 to an expected 1.5 million this year.[12] It is simply not cost effective to guard against all of these potential intruders.

In addition there are many other possible threats to a computer system's stored information and the continued successful operation of the facility itself. The first threats to be considered here are to data: accidental or intentional disclosure, modification or destruction.

There is a subtle difference between the modification and the destruction of data that managers must be aware of when planning for protection and subsequent recovery. Destruction is a visible, recognizable loss in which a file must be replaced from storage or completely regenerated. Modification is in itself quite devious. The file can appear to be intact and be perfectly usable, yet contain erroneous information. Accidental modification happens as a result of human keypunching/input errors. Intentional modification can be the basis for internal fraud and embezzlement which indicates a serious breach in security. Disclosure can be obvious (a file is removed from storage) or it can be concealed (information is copied by an outsider or disgruntled employee). In addition, program errors and employee mistakes

[12] "The Retailing Boom in Small Computers," Business Week (September 6, 1982): pg 92

can cause serious damage. Seemingly minor accidents can have severe consequences.

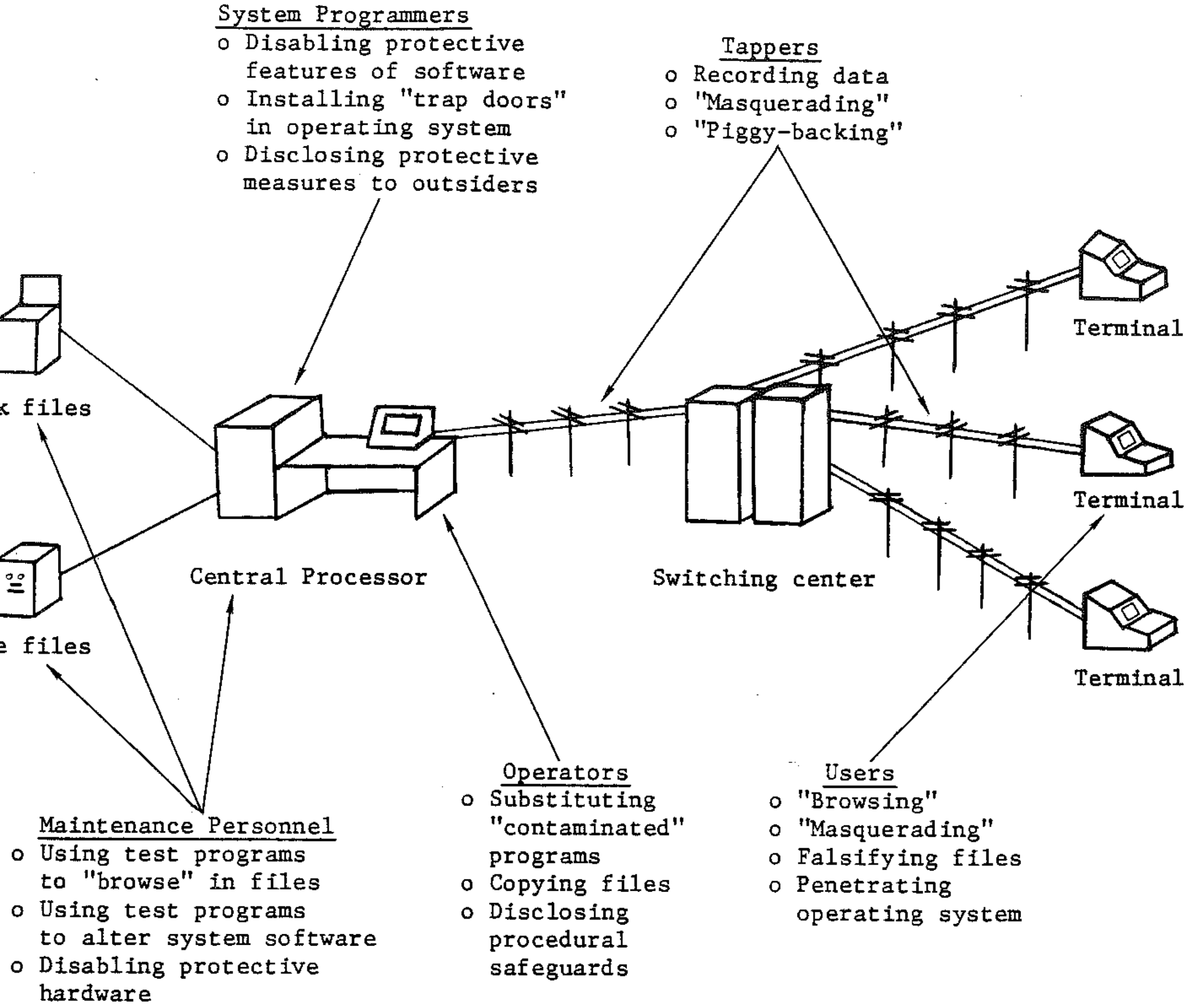
As Figure 1 indicates, a modern computer system is vulnerable to attack and penetration at many points along its information flow from a vareity of people both inside and outside of the organization. The motivation for such penetration may range from simple curiosity, to stealing the secret records of an individual or a competitor or causing the system to malfunction. System programmers, operators and maintenance personnel usually have the inside opportunity to penetrate system security and they may do so for personal grudges or personal gain.

Operators may have daily opportunity to tamper with data or files substituting their own programs. They can make duplicate copies of master tapes for outsiders in a few minutes or disclose the safeguards of a system. Programmers who write software can insert their own code into an operating system in such a way that it provides a "trap door" for penetration at any convenient time in the future. They can also identify programming techniques to outsiders. Maintenance personnel may incorporate subversive instructions into the test programs they use to test for malfunctions.

But even without this help from within the company, outsiders can gain access to the secret records stored in an organization's computer system. Among the techniques employed against online systems are "masquerading" and "piggybacking." Penetrators obtain the passwords of

FIGURE 1

THREATS TO THE INFORMATION PROCESSING SYSTEM


System Programmers
o Disabling protective features of software
o Installing "trap doors" in operating system
o Disclosing protective measures to outsiders
Tappers
o Recording data
o "Masquerading"
o "Piggy-backing"
Terminal
k files
Terminal
Central Processor
Switching center
e files
Terminal
Operators
o Substituting "contaminated" programs
o Copying files
o Disclosing procedural safeguards
Users
o "Browsing"
o "Masquerading"
o Falsifying files
o Penetrating operating system
Maintenance Personnel
o Using test programs to "browse" in files
o Using test programs to alter system software
o Disabling protective hardware

(Source: Tom Alexander, "Waiting for the Great Computer Rip-off," Fortune, Page 144, July 1974.)

legitimate users by wiretaps or various bugging devices and then use these passwords to masquerade as authorized users in order to obtain access to the system. Piggybacking is when a small computer terminal is attached to a tapped communications line where it may intercept and modify actual messages. Sometimes legitimate users borrow passwords to browse in other people's files.[13] Electronic devices are now available that will pick up electromagnetic radiations given off by computing equipment and convert these radiations into usable form. Also, material discarded as waste can be an important source of information.

Another consideration of computer security that will be taken into account deals with physically protecting the system against: sabotage, natural disaster, fire and water damage.

Sabotage can be directed against the entire system or just selected parts of it. This can range from willful destruction of important records by an employee, to the bombing of the computer center by terrorists. Damaging power lines will result in the disruption of the system. Natural disasters occur with some frequency in different parts of the country. Floods, tornadoes, hurricanes and blizzards are a few examples that can damage or completely destroy a computer system. Fires in data processing equipment usually have a common beginning. Electrical equipment fires are

[13] Tom Alexander, "Waiting for the Great Computer Rip-Off," Fortune (July 1974): pg 145.

characterized by a breakdown of insulation and a resulting short circuit. The heat can become intense and generate large amounts of smoke. In many nonelectrical fires, water is used to extinguish the blaze. Water usually causes more damage than the fire it contained. "Water can be particularly damaging to electronic components, wires, and cables."[14] At least, the equipment cabinets would have to be dried thoroughly before power was reapplied. At worst, the water could cause additional short circuits when power is reapplied. The resulting clean-up will cause additional delays in getting the system online again.

We will now examine two different companies, one which was a victim of computer crime and another which has implemented the latest techniques to protect itself.

The first company to be examined is a medium-sized bank having several local branches within a small city. A centralized computer system is on-line, having remote terminal access and using a standard savings account software package. The remote terminals can be locked at night when not in use, but it is the bank's practice to leave them unattended. The computer operator functions independently of the programmer, although the programmer has access to live data files. The operator is not a programmer and is not familiar with programming.

[14] Donald H. Sanders, "Computers in Society," (McGraw Hill, Inc., 1977): pg 261.

The perpetrator in this incident worked at night as a programmer for the bank. Due to his increasing personal financial difficulties, he decided one night to transfer $100 from forty-one different savings accounts into a new one that he had opened. His wife withdrew the money over several days. A short time later, a controller's friend called him to report a discrepancy. The perpetrator and his wife were apprehended.[15]

In summary, there are many reasons a fraud like this was allowed to occur. First, new employees were never screened. Neither background nor credit checks were accomplished. Second, programmers were allowed access to terminals after hours. This is an example of the failure to maintain a separation of duties between personnel and unrelated jobs. Third, there was a lack of a monitor control function, no one checked the programmers work from the night before.

Now we will examine a company which has taken effective measures to prevent computer crime. McDonnell Douglas Automation Company, MCAUTO, a division of McDonnell Douglas Corporation, contains more than 105,000 square feet of raised-floor computer space. The temperature and humidity of the computer areas are controlled to maintain the equipment's operating efficiency. Humidity is controlled to reduce static electricity. All fire codes were met on the

[15] Donn B. Parker, "Crime by Computer," (Charles Scribner's Sons, 1976): pg 175

design of the facility. Fire prevention is enhanced by smoke and heat sensors located throughout the facility. Computer rooms are equipped with fire extinguishers. A sprinkler system, and a fire alarm system are installed. MCAUTO has security guard protection at all access points, twenty-four hours a day, seven days a week. All employees are required to wear photo badges. Visitors are escorted at all times.[16]

This is an example of a company that has the financial ability to employ the latest techniques in preventing computer crime.

Summary of Chapter 2

The computer, initially developed for the Army in 1944, was incorporated into the commercial business field ten years later. Today, the computer's influence can be seen almost everywhere.

Computer crime is a very real threat to the successful operation of a company's system. This threat can come from a number of sources, both inside and outside of the company and be in the form of trusted employees to saboteurs. This is why it is imperative that the security of the computer system remain the data-processing manager's top priority.

In addition, two separate companies were examined. First, a medium-sized bank that suffered a loss and second, a large company that is trying to prevent a loss. In

[16] "Physical Security and Administrative Safeguards," (McDonnell Douglas Automation Company Report N0627-062, June 1982): pg 28

Chapter 3, protective measures for the various threats to a computer system will be examined along with the advantages and limitations of each measure.

CHAPTER III

Methodology

The information collected for this study will be analyzed in a variety of methods. Since the purpose of this study is to assist a data-processing manager in deciding whether or not he can adequately protect the company's medium-sized computer system, a model will be built. This model will outline the advantages and limitations of the various protective measures presented in this study. The data-processing manager will be employed as a hardware wholesaler suppling several local retailers and has responsibility for the secure operation of the company's UNIVAC 1110 computer system. The manager will monitor the physical security of the system along with inventory control, personnel files and financial records.

There is a large variety of medium-sized commercial computers available on the market today and many of these systems are relatively the same. The UNIVAC 1110 was selected because it was designed for simultaneous batch, remote batch, time-sharing and real-time data processing in a wide variety of applications.[17] Its features include extensive memory capability, a central processor and an operator's console for input, error correlctions and two-way communication with

[17] Boulton B. Miller, "Computers, A User's Introduction," (Bainbridge Inc., 1974): pg 222.

the computer. It can accept data from a number of sources; magnetic disks, magnetic tapes, printer unit and cathode-ray tube (CRT). It can also accommodate several remote terminals for communication with branch offices.[18]

The security threats to this computer system have been presented. This was used to show the manager the variety of different threats he has to protect against. The manager wants to maintain a cost effective security program for his computer system. To accomplish this objective, he must be able to counter every threat, both internal and external without the use of expensive techniques. The advantage of using cost effective methods is that the manager will be able to apply these to other comparable computer systems. This allows the manager to maintain a flexible response to any additional threats which may occur.

Should a theft take place, this paper will discuss some of the legal ramifications of computer crime. Finally, the future will be examined and the threat of computer crime considered.

Analysis

The manager must insure good security principles are practiced both inside and outside of the company's walls. Recognizing that a threat exists is the first step in

[18] S. J. Wanous, G. E. Wagner and S. F. Hallam, "Introduction to Automated Data Processing," (South-Western Publishing C9., 1979): pg 8.

protecting against it. Many devices on the market today enable companies to scramble codes, monitor telephone calls and limit access to data. Threats have been presented both from internal and external sources. A loss resulting from the penetration of any one of these sources, could result in millions of dollars. An operator falsifying inventory records so that they appear correct while his partner steals inventory off the shelf, or a programmer adding a little something extra to his paycheck each week are examples of what the data-processing manager has to protect against. We will now examine how the manager can effectively protect the computer system from these threats.

The location of a computer installation can itself be a means of achieving an acceptable level of security. In an established facility, it may be possible to take advantage of present security measures already in practice. If there is some type of perimeter control, the first line of security already exists. The chance of direct sabotage is now lessened. Disruption of power and communication lines might be prevented because specific lines would be difficult for the saboteur to isolate. Eavesdropping becomes almost impossible in a large complex with an adequately patrolled perimeter. A computer installation in a separate building makes it easier to control building access but it is also more vulnerable to isolate and direct attack.

protecting against it. Many devices on the market today enable companies to scramble codes, monitor telephone calls and limit access to data. Threats have been presented both from internal and external sources. A loss resulting from the penetration of any one of these sources, could result in millions of dollars. An operator falsifying inventory records so that they appear correct while his partner steals inventory off the shelf, or a programmer adding a little something extra to his paycheck each week are examples of what the data-processing manager has to protect against. We will now examine how the manager can effectively protect the computer system from these threats.

The location of a computer installation can itself be a means of achieving an acceptable level of security. In an established facility, it may be possible to take advantage of present security measures already in practice. If there is some type of perimeter control, the first line of security already exists. The chance of direct sabotage is now lessened. Disruption of power and communication lines might be prevented because specific lines would be difficult for the saboteur to isolate. Eavesdropping becomes almost impossible in a large complex with an adequately patrolled perimeter. A computer installation in a separate building makes it easier to control building access but it is also more vulnerable to isolate and direct attack.

Once the building is selected, access control to the facility must always be maintained. This can be done in several ways. Limiting the number of building entrances is an important control method. In addition, issue and require display of photo ID badges that are visually coded for immediate personnel recognition.[19] Some installations were designed as glass-walled showcases allowing a great deal of outside visibility into the operations area. Such accommodations offer little protection from outsider observation. All doors and walls should be solid to prevent covert observation. Locations inside the building are preferred over those along outside walls, because of exposure to external hazards. Upper floor locations would also be easier to protect. Locating a data-processing center below ground level should be discouraged because of the chance of water damage from, broken water lines, flooding, sewer back-up and heavy rains.

Many techniques exist for controlling limited entry into the computer room. Special combination locks, monitored double door entry and guarded entrances are all very effective. Guarded entrances are probably the most popular because it allows for the escorting of visitors and maintenance personnel. In addition, a log of entrance activity can be maintained which indicates the individual, reason for entry and

[19] "Crime in Service Industries," U.S. Department of Commerce (September 1977): pg 120.

authorization. Every briefcase and container which is brought into the area can easily be inspected by the guard. CRT's cannot be left out in the "open" but should also be subject to access control. Any waste paper generated inside the computer room must be handled as classified waste and disposed of within the room.[20] This is best accomplished by a shredder or depositing the material into a security container.

Fire prevention is an important part of protecting the computer facility. The facility should be fireproof, including the raised floor, suspended ceiling and air conditioning ducts. Good housekeeping and cleanliness are vital to maintaining a noncombustible environment. Hand-held extinguishers should be spaced around the operations area so that they are clearly visible and readily accessible. A sprinkler system can also be installed.

Water damage is a potential problem that should be protected against. All outlets, telephone lines, cables and doors should be sealed in a way to maintain the integrity of the room. Fitted plastic covers should be attached to each console, to be applied in the advent of inadvertant sprinkling. As an added feature, if economically feasible, the room and cabinets of the computer screens and keyboards could

[20] Ibid.

be lined with steel to muffle electronic translations.[21] Any security procedures implemented at the computer center must also be implemented at every user terminal located at each remote branch office. This in itself may be difficult, because remote terminals could be located several hundred miles away. If necessary, the manager may appoint an assistant security monitor at each branch office who would insure security procedures are being carried out.

Even the storage facility, commonly referred to as the disk/tape library must be guarded constantly to prevent unauthorized entry. Maintenance personnel and programmers should not be allowed free access to these files in storage. Maintenance of the library should be by an assigned individual. All tapes and disk packs should be clearly labeled as to their contents. Type of data can be indicated by number, type or color. This makes identification readily visible to all. An audit trail of all data usage should be kept. Information should include, dates on which tapes/disks entered the library, to whom and when they have been checked out, who authorized it and for how long. The data-processing manager must always insure that access control to every aspect of the information processing system is maintained. The physical security concepts have been discussed in detail and are listed in Appendix A. Software security will now be examined.

[21] "Preventing "War Games"," Newsweek (September 5, 1983): pg 48.

The greatest threat to software security are the people who work with the programs. Protecting the system from personnel penetration is a continuing process. First, the manager must decide on the role of the data processing department, whether it is going to be a separate service center or subordinate to another department. The type of installation, experience level of employees and demands for services usually determines this. Once this is established, an organizational chart and job description showing each employee's position and responsibilities should be distributed. It is the manager's responsibility to insure that there is always a separation of duties between personnel. "Functions of programming, operating and controlling must be separated. No programmer should have access to the computer. His function is design - not operation. Control must be independent of operators."[22] This will help insure that system integrity remains intact.

Aside from the concern with adequate separation of duties, the manager should also be concerned with the quality and quantity of staff and the stability of the employees. There should be a sufficient number of people with experience to handle the work, both in processing data and designing new programs. A high employee turn-over rate is an indication of a serious morale problem. Once the decision

[22] "Crime in Service Industries," U.S. Department of Commerce (September 1977): pg 121.

to "remove" an employee is made, immediately terminate his access to the computer system. Regardless of the reason, he must not be allowed further entry, the risk of sabotage is too great.

As the requirements of the computer center increase, more data will be processed and distributed over several departments. When this situation exists, there is a need to establish a data base administrative function. An individual would be appointed to monitor the ways in which data is to be used. This would protect the integrity of various data elements from rival departmental tampering. When departments share programs, it is essential that they all understand the size of the program, format, meaning and characteristics. This will help maintain a smooth flaw of information. Program changes are the responsibility of the data base administrator. Nearly all systems need occasional revisions to meet changing requirements or to improve their usefulness. The most effective method, in terms of control, is to require all program changes to be treated as seriously as new programs which includes, formal authorization, approval, and testing. The entry for data base changes will be made in a separate data file. This file contains one entry for each change that is made to the data base and one for each transaction. The entry for the change points to the terminal it originated from. This allows the operator to be identified. Thus, every change to the data base can be traced back to the person responsible. Another method to protect computer programs is through a copyright.[23]

One of the main defenses against computer crime today is the use of passwords. These secret codes allow access to the computer's data. Passwords, as a result of employee indifference, often turns out to be a laughable defense. "Passwords are a weak defense against the computer snoop, Leibholz said. Like the programmer in "War Games," many people choose the names of their spouses, children, birthdays or social security numbers as passwords. Others paste the magic word on their computers where they won't forget it. or use an easily remembered name."[24] This is the kind of careless attitude the manager must protect against. Passwords are effective when used properly. They should be changed frequently and on an irregular basis so as not to establish a pattern.

As an added precaution, a copy of each tape, disk, file should be made and treated like a master to be placed in a separate, secure building. This could become expensive as the scope of computer operations increase. Budget constraints may warrant this as impractical.

[23] Boulton B. Miller, "Computers, A User's Introduction," (Bainbridge Inc., 1974): pg 32.

[24] "Theft By Computer Is On The Rise," St. Louis Post-Dispatch (September 6, 1983): pg 15A.

The best and most expensive defense against computer wiretapping is achieved through the use of encryption/decryption devices. The encryption device turns electronic data from the computer center into gibberish, so if it is intercepted over the telephone lines by an outsider, it will be of no usable value to him. At the branch office, a decryption device turns the gibberish back into usable information. This process reverses itself when the branch office sends the computer center information. Says Donn Parker of SRI International, a California research firm:

> "Encryption is the control of the future. During the '80s it will become very important."[25]

The data security concepts have been discussed in detail and are listed in Appendix B.

The Law

Once a computer crime is committed, the legal recourse can be more frustrating than the crime itself. In 1974, only 42% of the states had effective laws against the theft of software and 24% for theft of computer time.[26] Since then, very little has changed. These laws only apply if the crime is committed within the state, interstate theft is handled by the federal government. Current federal laws are inadequate, confusing and limited. August Bequai, a criminal

[25] "Crackdown on Computer Capers," Time (February 8, 1982): pg 61.

[26] R. P. Bigelow and S. H. Nycum, "Your Computer and the Law," (Prentice-Hall, Inc.): pg 166.

lawyer who served as chairman of a Federal Bar Association subcommittee on whitecollar crime, told Editorial Research Reports that the chance of an electronic crime being discovered is only one in a hundred.

> "And the likelihood of being convicted of a computer crime is one in five hundred and of going to jail one in a thousand. The odds for avoiding a stiff sentence are even more favorable."[27]

The Future

Protecting the computer system will be even more important in the future. Businesses will continue to automate as much as possible to make it easier for themselves and the consumer. More and more information will be flowing over telephone lines. Encryption and decryption techniques will have to be perfected and expanded to incorporate all systems. The threat from outsiders will only increase. John Ganty, vice-president of International Data Corp. is forecasting 2.8 million unit sales annually in the U.S. by 1985, while Clive C. Smith, an analyst at the Yankee Group, sees sales as high as 8.8 million units - of which 6.5 million will be home computers - for that same period.[28]

[27] Eric Oatman, "Crime and Society," The Reference Shelf (H. W. Wilson Co. 1979): pg 90.

[28] "The Retailing Boom in Small Computers," Business Week (September 6, 1982): pg 97.

State and federal laws must be improved to help deter computer crime. Without the valid threat of prosecution, computer crime will reach epidemic proportions in the future.

Summary of Chapter 3

In Chapter 3, the various protective measures against computer crime have been presented. These measures can be applied to threats from both internal and external sources. The data-processing manager must take an active role in preventing computer crime. Chapter 4 will summarize what has been covered, draw conclusions and look at implications for further study.

CHAPTER IV

Conclusions

Computer crime is a very real problem that must be protected against. Protective measures vary depending on the specific threat. The most common method to physically protecting a computer system is with guarded entrances. The most effective method to protect against wiretapping is to install encryption/decryption devices at all of the facilities. This however, could be too costly for a small company.

The data-processing manager must take an active roll to insure all the security procedures are being followed. The computer facility and the data inside of it can be protected in a way which minimizes the chance of penetration. However, no facility, regardless of the methods employed, can be made totally secure from a determined hostile force.

Summary

Today, many companies have incorporated some form of data-processing in their daily business transactions. This has improved the flow of information within the company. Monotonous jobs can now be processed quickly and more efficiently.

There is, however, a problem. Computer crime effects us all. The actual dollar losses are impossible to calculate. Accurate statistics are unavailable because many thefts are never reported. Threats to a company's computer system can be from either internal or external sources. They can be in the form of sabotage, flood, fire, wiretapping or many others.

Companies regardless of their size must protect against this crime. Small companies feel that it would not happen to them, but it does and at an alarming rate. Large companies which have substantial financial resources, must utilize these wisely to guard against intrusion.

There are many techniques available to help protect against these threats. Guarded entrances, sprinkler system, encryption/decryption devices, photo ID badges are just a few which are available. Each preventive measure must be examined thoroughly before it is implemented because of its advantages and limitations. Should a crime occur, there is little legal recourse for a company to take. Current laws are inadequate and in need of revision.

Implications for Further Study

This study concentrated on a medium-sized computer in the business environment. A study could be conducted focusing on computer abuse within government institutions. Since the government maintains files on millions of people, the study could emphasize a person's right to privacy and if the government is adequately protecting it. Recently, intruders have successfully penetrated several military computer systems. A study concerning the precautions the military takes to prevent computer abuse would be beneficial. This could be defined even further by examining either physical or data precautions.

The protection of software was discussed, but a different study concentrating on the actual programs and how they could be written to help prevent computer crime could be accomplished. The technical aspects of the program would be examined and recommendations to improve the programs made.

A study based on actual computer crimes and the resulting prison term served would be an indication of how effective the current laws are. This study would examine the federal, state and local laws, their enforcement and conviction rate.

APPENDICES

APPENDIX A
RESPONSES TO PHYSICAL THREATS

THREAT	RESPONSES	ADVANTAGES	LIMITATIONS
ect outsider sical sabotage	24 hour perimeter control	a "show of force" to discourage attack	continual manpower costs
		constant patrolled area	larger the area, less effective
	upper floor location of computer facility	increased difficulty to break-in to	
uthorized access building	computer facility in separate building	effective control over building access	easier to identify and electrically isolate
	limit building entrances	maintain control of employee and visitor activity	creates bottleneck during rush hours
	issue coded/photo ID cards for entry	immediate recognition of all authorized personnel	segregation of employees by job
ert observation operations	insure walls and doors are solid	prevents observation of computer operations	employees have a feeling of isolation
	place computer in separate area	enhances ability to protect facility	limits access to employees
			creates paperwork backup
uthorized entry facility	combination locks	prevents inadvertent entry	initial installation cost
			combinations can be compromised
	monitored double door entry	allows area to challenge intruders	initial cost
			guards required
	guarded entrances	allows for positive identification	continual manpower costs
		ability to escort visitors	
		able to search containers	
		maintain a log of activity	

THREAT	RESPONSES	ADVANTAGES	LIMITATIONS
ttended s	control of CRTs	prevents unauthorized usage	limits availability to employees
carded uments	shred within facility	immediate destruction of unwanted information	initial purchase cost
	deposit in container	saves employee's time	trust guard to destroy info
e	original building construction	incorporate modern firefighting techniques	initial building cost
	extinguishers	immediate response to fire	limited applicability
	sprinkler system	complete area coverage	water damage
er ge	seal room	insures integrity of room	initial cost and maintenance
	plastic covers	inexpensive	slow to apply

APPENDIX B

RESPONSES TO DATA THREATS

THREAT	RESPONSES	ADVANTAGES	LIMITATIONS
pering h tapes	limit accessability	prevents unauthorized usage	instills sense of mistrust
	label data	data clearly marked	
	establish audit trail	maintain record of tape usage	increase paperwork
	appoint data base administrator	acts as intermediary between departments	must trust administrator
	frequent password changes	increases difficulty in penetrating system	employee confusion
	duplicate all tapes	one complete set of master tapes	continual maintenance cost
	strict policies regarding changes	insures changes are correct	increased paperwork
	copyright	official recognition	little practical value
efined role employees	establish administrative guidelines	clear supervisor/ employee relationship	limits flow of communication
		job description and responsibilities defined	
minated loyee	terminate access to computer	prevents sabotage	
promised sword	frequent password changes	increased difficulty in penetrating system	confuses employees
etapping	encryption/ decryption devices	completely scrambles data	initial purchase and installation cost

BIBLIOGRAPHY

Newspapers

"Theft by Computers Is On the Rise," *St. Louis Post-Dispatch* (September 6, 1983), pg 15A.

Periodicals

Alexander, Tom. "Waiting for the Great Computer Rip-Off," *Fortune* (July 1974), pg 143-152.

"Beware: Hackers at Play," *Newsweek* (September 5, 1983), pg 42-48.

"Crackdown on Computer Capers," *Time* (February 8, 1982), pg 60-61.

"Physical Security and Administrative Safeguards," McDonnell Douglas Automation Company Report N0627-062 (June 1982), pg 28-29.

"The Computer Moves In," *Time* (January 3, 1983), pg 14-39.

"The Retailing Boom in Small Computers," *Business Week* (September 6, 1982), pg 92-97.

"When Criminals Turn to Computers, is Anything Safe?" *Smithsonian*, (August 1982), pg 117-126.

Books

Bibby, Dause L., *Your Future in the Electronics Computer Field*. New York: Richards Rosen Press, 1970.

Bigelow, Richard P. and Nycum, Susan H., *Your Computer and the Law*. New Jersey: Prentice-Hall, 1975.

Diebold, John, *The World of the Computer*. New York: Random House, 1973.

Jacket, Corinne, *Man, Memory and Machines; An Introduction to Cybernetics*. New York: The MacMillan Company, 1964.

Lukoff, Herman, *From Dits to Bits: A Personal History of the Electronic Computer*. Oregon: Robotics Press, 1979.

Miller, Boulton B., *Computers, A User's Introduction*. Bainbridge Inc., 1974.

Oatman, Eric, *Crime and Society, the Reference Shelf*. New York: H. W. Wilson Company, 1979.

Parker, Donn B., Crime by Computer. New York: Charles Scribner's Sons, 1976.

Price, Wilson T., Introduction to Computer Data Processing. Hinsdale: The Dryden Press, 1977.

Sanders, Donald H., Computers in Society. New York: McGraw Hill Inc., 1977.

Walsh, Myles E., Understanding Computers: What Managers and Users Need to Know. New York: John Wiley & Sons, Inc., 1981.

Wanons, S. J., Wagner, G. E. and Hallom, S. F., Introduction to Automated Data Processing. Cincinnati: South-Western Publishing Company, 1979.

DAKOTA BOOKBINDING
116 - 2nd Street N.W.
Mohall, ND 58761
Telephone: 756-7151

658.478
D691

Doonan, Michael J.

Protecting the medium-sized business
computer

DATE DUE

658.478
D691

AUTHOR

Doonan, Michael J.

TITLE Protecting the medium-sized
business computer

DATE DUE	BORROWER'S NAME
~~14 MAY 85~~	~~CARBAJAL~~
4/23/82	Nelson
9/25	''

PROPERTY OF THE U.S. AIR FO
Air Force Institute of Technology
Library
Minot Air Force Base