CONFRONTING COMPUTER CRIME: A CHALLENGE FOR THE 1980s

Report
of the
Computer Security Subcommittee
of the
Metropolitan Council's
Criminal Justice Advisory Committee

April 1984

Metropolitan Council of the Twin Cities Area
300 Metro Square Building, 7th and Robert Streets
St. Paul, Minnesota 55101
Tel. (612) 291-6359

Publication No. 36-84-046

COMPUTER SECURITY SUBCOMMITTEE

Susan Gray, Chair, Attorney

Dennis R. Berry	Investigator, Hennepin County Attorney's Office
James R. Coleman	Chair, Computer Law Committee, Hennepin County Bar Association
John D. Erskine	Superintendent, Bureau of Criminal Apprehension
Marr T. Haack	Commercial Properties Underwriting, The St. Paul Companies, Inc.
John Hawksford	Vice President, Marketing, ROI Systems
Robert Huber	Computer Systems Coordinator, Minneapolis Police Department
John P. O'Connor	Supervisor, White Collar Crimes Division, Federal Bureau of Investigation
Paul D. Porter	Data Services Security Manager, Control Data Corporation
James Rosenbaum	United States Attorney
Allen Stendahl	Regional Underwriting Manager, The St. Paul Companies, Inc.
Thomas F. Sullivan	Director, Financial Investigations, Attorney General's Office

Donna Mattson, Metropolitan Council Staff

TABLE OF CONTENTS

SUMMARY

With computers playing a key role in the day to day activities of Metropolitan Area businesses and citizens, there is growing concern about the potential for computer-related crime and the availability of resources to effectively handle the problem. Although precise statistics about the extent of computer misuse are not readily available, indications are that losses resulting from computer crime are substantial. Also, with the growing sophistication of computer users and the often minimal computer security, the potential for increasing misuse is great. It must be viewed as a serious concern for both the business community and the resources of the criminal justice system.

In 1982, the Minnesota legislature passed a law that specifically addresses computer-related crime, but there are still a number of legal issues related to this topic which need further examination.

Laws alone cannot protect against this problem. There is also a need for greater public awareness about the issues and ways they can be addressed. Schools can play a key role in educating young people about the personal and legal ramifications of computer misuse. In addition, professional networks with members involved in working with computers or in addressing computer crime issues can facilitate the exchange of information about computer security and the resources available for handling the problem.

Increased coordination and cooperation between businesses and law enforcement agencies is also needed. The criminal justice system cannot deal with crimes that it does not know about. Factors that inhibit the voluntary reporting of computer offenses must be examined.

In addition, businesses should increase their efforts to prevent and control computer crimes. Top management has to take increased responsibility for implementing and maintaining security. Company officials must be better educated about computer system vulnerability and safeguard options. They must also play a key role in examining security controls on a regular basis.

While efforts to address computer security issues are increasing, the need for continual examination of the problem has not diminished. With the rapid advances in computer technology, there is a need to identify new problem areas and resources needed. It is therefore important that groups continue to work together to coordinate resources and share information on this topic.

This report is intended to stimulate discussion of some of the major issues and to facilitate coordination of resources in addressing the problem of computer-related crime in the Twin Cities Metropolitan Area.

INTRODUCTION

Computer technology has dramatically altered modern society. Most companies and businesses now rely on computer systems for handling their major work functions. Computers also play a key role in the day-to-day transactions of almost every individual citizen.

The changing technology has also brought about the development of a new area of white collar crime--the misuse of computers. There are new ways of committing crimes because of the changing forms of assets, such as funds transferrable through telephone lines. In addition, crimes can now be perpetrated within a fraction of a second, crossing many jurisdictional lines and covering vast distances.

Until recently, most individuals were intimidated by the mystique of computers. Now, however, more and more people are being trained in the use of new technologies and there is increasing experimentation with computer system capabilities. The movie "War Games" illustrated the potential impact of such experimentation. Future generations will be even better prepared to work in a computer-oriented environment and the potential for computer misuse will increase significantly. For these reasons, it is imperative that planning efforts be directed now at addressing the issue of computer security so that appropriate preventive action can be taken.

ESTABLISHMENT OF A COMPUTER SECURITY SUBCOMMITTEE

The rise of computer technology has created circumstances and situations that could not have been anticipated by the criminal justice system. As a result, there is concern about whether or not the existing criminal justice system and its resources are adequate to address the problem of computer-related crime.

As the only metropolitan agency with responsibility for examining problems that transcend municipal and county boundaries, the Metropolitan Council seemed to be an appropriate agency to study this problem. The Twin Cities Area serves as corporate headquarters for a number of businesses directly involved in the development and use of computers and related technologies. In addition, federal, state, and local criminal justice agencies in the region have a history of working in a coordinated and cooperative manner on issues of mutual concern.

In June 1982, a subcommittee was appointed by the Council's Criminal Justice Advisory Committee to examine the problem of computer crime in the Metropolitan Area. The twelve-member subcommittee had representatives from federal, state, and local investigation and prosecution agencies as well as from the computer, banking and insurance industries.

The Computer Security Subcommittee was assigned and directed to:

1. Engage in a cooperative effort with private industry and federal, state and local law enforcement agencies to seek ways to improve the prevention, detection, investigation and prosecution of crimes involving the use and abuse of computers and related communications technology.

2. Recommend to the full committee strategies for preventing and controlling these crimes.

3. Assist appropriate public agencies and private industry with the implementation of adopted strategies.

The subcommittee met 14 times while gathering information for this report. An orientation meeting was held to provide subcommittee members with background information on the development and enactment of the Minnesota computer crime law (see Appendix, page 20). Individuals involved in drafting of the legislation presented the subcommittee with an overview of the issues and the process used in the bill's preparation. The subcommittee also held a series of meetings at which representatives of the legal profession, the computer industry, auditing firms and law enforcement agencies were present to discuss various aspects of the problem.

The subcommittee was then divided into two groups to examine private sector and public sector roles in addressing the problem of computer crime. Members were assigned to a group based on their specific knowledge or interest in particular aspects of the problem. Each group identified specific issues to be addressed. These were then considered by the full subcommittee in preparation of the final report.

The report was distributed for public review and comment, and two public meetings were held. The subcommittee then revised certain portions of the report to address concerns raised through this process. The report was presented to and accepted by the Metropolitan Council on April 12, 1984.

The recommendations contained in the report were agreed on by subcommittee members and do not necessarily reflect the opinion of the businesses or agencies they represent.

The subcommittee acknowledges the assistance of the following people who contributed to the development of this report:

Pete Connors, Hennepin County Attorney's Office
James Dixon, Compu-Tel International
Tom Fable, Minnesota Attorney General's Office
Terry L. Gruzebeck, intern, Hennepin County Attorney's Office
Hans W. Herb, intern, Hennepin County Attorney's Office
Cort Holton, Chestnut and Brooks, P.A.
Ron Kaatz, Federal Reserve Bank
Phyllis Kahn, State Representative
Rita Kaplan, Honeywell, Inc.
Bill Korn, Minneapolis City Attorney's Office
Doug LaChance, ITT Consumer Financial Corporation
Jerry Lee, Norwest Audit Services
Clarence M. Lewis, Compu-Tel International
Mike Miller, McGladrey Hendrickson and Company
John Nugent, Norwest Information Services
Lawrence A. Parks, Ernst and Whinney

Robert Peterson, Bloomington Public Schools
Stan Whittingham, Farmington Police Department
William Wurster, Federal Reserve Bank
Steven Zachary, intern, Metropolitan Council
Robert Zeller, Minnesota Cable Communications Board

RECOMMENDATIONS

Major recommendations contained in this report include:

1. The extent of the computer crime problem in the Twin Cities Metropolitan Area must be examined further because accurate information on this problem currently is not available.

2. Current Minnesota law specifically addresses computer-related crime, but there are related legal issues which require further examination. These include: the need for provisions in the law to cover the aggregation of computer thefts; extending the statute of limitations; clarifying civil liability in computer crimes; defining jurisdiction for prosecution; departing from the sentencing guidelines; controlling the information put on electronic bulletin boards; penalizing "attempts" to access computer systems; and modifying the statute to deal with "unauthorized use" of computers.

3. Security education efforts aimed at the prevention and detection of computer misuse must be increased.

4. Schools should incorporate into their computer literacy curriculum ways of heightening awareness of the legal and personal ramifications of computer misuse. School personnel should also share curriculum information on this topic with other schools through existing networks in an attempt to sensitize the educational system to the need.

5. Greater management control of in-house computer systems is needed. Top management must be better educated about computer system vulnerability and safeguard options. They must also play a key role in examining security controls on a regular basis.

6. Detection and reporting of computer misuse are major problems to be addressed. More resources need to be dedicated to the detection of misuse. There is also a need to further examine the factors inhibiting voluntary reporting of computer offenses.

7. Increased communication and sharing of information and resources between businesses and law enforcement agencies is needed in the handling of computer-related offenses.

8. The computer can be a valuable investigative tool for law enforcement personnel. Law enforcement agencies should be further trained in the capability and availability of computer systems for investigative work.

9. Specialized training in computer crime issues is essential for law enforcement personnel involved in the investigation of white collar crimes.

10. The role of private security personnel in controlling computer crime or misuse should be increased.

11. The insurance industry will play an increasingly important role in the management of the risk of theft by computer. As loss from computer thefts increases, underwriters will require effective management controls as a prerequisite for providing computer theft coverage. In order to create an awareness of the risks associated with increased dependence on computers, insurers will need to share information with each other as well as with other agencies.

12. Special attention should be paid to the computer security needs of small businesses and first-time computer users.

13. An ongoing computer security task force should be established to coordinate the distribution of information on computer security issues affecting the Twin Cities Area.

SCOPE OF THE PROBLEM

Although there are many reports of computer-related crimes, the actual number and frequency of such crimes and the losses resulting from them are unknown. This is because many computer-related offenses go undetected. And even when detected, they may not be reported outside the organization.

Media reports strongly suggest, however, that computer crime and misuse do occur regularly. Furthermore, the potential for increasing levels of computer misuse and fraud is great due to the increasing use of computer technology, the greater number of computer users, the rapid growth in the number of skilled computer personnel, and the fact that computer security is often minimal. For these reasons, computer crime must be viewed as a serious concern for both the business community and the resources of the criminal justice system.

The subcommittee's study showed that some of the unique features of computer-related crimes include:

- The losses resulting from such crimes can be very large. The U.S. Chamber of Commerce has estimated that computer crimes cost businesses well over $100 million annually. Other sources estimate the annual loss from such crimes may be as high as $3 billion.

- Businesses and financial institutions are not the only victims of computer crime. When a business suffers a monetary loss--like that of shoplifting--the cost is at some point passed on to the consumer. It is estimated that all white collar crime adds 15 percent to the cost of retail goods.

Personal lives of citizens can also be affected by misuse of computers. If monetary records or credit reference data is tampered with, one's ability to cash a check or to obtain credit can be affected. If one employee alters another employee's work, the second person's work record can be affected. There is also a possibility that medical and academic records can be altered through computer misuse.

- Considerable sensitivity surrounds reporting such offenses. Victims have been reluctant to report computer crimes because they may fear adverse publicity and loss of confidence in their companies.

- Computer-related crimes are extremely difficult to detect. These crimes are usually not readily visible, and even when detected, it may be difficult to determine how the offense was committed.

- A large proportion of computer crimes are committed from "within" a business or organization. Because the chances of discovery are minimal, temptations exist for employees who have access to computer systems to manipulate them for personal gain.

- The individuals who commit computer-related crimes range in sophistication from the entry level clerk to the skilled computer expert.

- The computer criminal is not always out for personal gain. There are those individuals who are challenged by computer system safeguards and work to "beat the system."

- Often with computer-related crimes, it is difficult to obtain physical evidence since information can be quickly altered or destroyed.

- The jargon of computer technology is difficult to translate into terms which everyone understands. As a result, the preparation of a computer crime case which can be easily understood by judges and jurors is a challenge for prosecution agencies.

- Money has changed from what is commonly thought of as cash into data in a computer system, the electronic funds transfer networks. In fact, it is estimated that in excess of $400 billion is transferred electronically each day in the United States.

All of these factors must be considered in dealing with computer crime. The business community (i.e., businesses, government agencies, and institutions that use computers for technical and business purposes) and criminal justice agencies are increasing their abilities to address this problem. It is necessary not only to develop new expertise in this area, but also to establish strategies for effective cooperation and coordination among all disciplines concerned.

DEFINITION OF COMPUTER CRIME

There is no universally accepted definition of computer-related crime. There seems to be agreement, however, that most computer-related crimes directly involve the use of a computer to commit acts which the law has already defined as criminal, such as theft of money, services, or property, invasion of privacy, extortion and sabotage.

Minnesota's computer crime law (see Appendix) provides the following definitions for acts of computer damage and computer theft:

> Whoever does any of the following is guilty of computer damage:
>
> Intentionally and without authorization damages or destroys any computer, computer system, computer network, computer software, electronically processed or produced data and information contained in a computer or computer software.
>
> Intentionally and without authorization and with the intent to injure or defraud alters any computer, computer system, computer network, computer software, electronically processed or produced data and information contained in a computer or computer software.
>
> Whoever does any of the following is guilty of computer theft:
>
> Intentionally and without authorization or claim of right accesses or causes to be accessed any computer, computer system, computer network, or any part thereof for the purpose of obtaining services or property.
>
> Intentionally and without claim of right and with intent to permanently deprive the owner of possession, takes, transfers, conceals or retains possession of any computer, computer system, or any computer software or data contained in a computer, computer system, or computer network.

COMPUTER CRIME LAWS AND OTHER LEGAL ISSUES

Although there has been considerable congressional discussion on this topic, no federal law currently in existence specifically addresses the problem of computer crime. One bill, recently introduced in Congress, is entitled "The Federal Computer Systems Protection Act of 1983." It would make it a federal offense to tamper with the computers of the federal government, the computers of financial institutions guaranteed by the federal government and computers operating in interstate commerce or using interstate facilities. Such activities would be punishable by fines of up to $50,000 or twice the value of the property stolen, imprisonment for up to five years, or both.

In 1978, Florida became the first state to pass legislation specifically addressing computer crime. To date over 20 states, including Minnesota, have passed computer crime laws.

Minnesota's computer crime law, passed during the 1982 legislative session, defines computer theft and damage and includes penalties for offenders. The enactment of this law makes it clear that certain acts involving use of a computer are criminal. Under the law, anyone who intentionally damages or alters computer hardware or software with intent to defraud could be sentenced to a maximum of ten years in prison and a $50,000 fine if the damage is put at more than $2,500. The actual sentence, however, is dependent upon the application of the state's sentencing guidelines.

The maximum penalty is the same for anyone found guilty of unauthorized use or theft of computer equipment, software or time worth more than $2,500. Both the theft and damage provisions carry less severe penalties for losses valued at less than $2,500.

Computer crime, when it has been discovered, has previously been prosecuted under theft, larceny, bank fraud, mail or wire fraud statutes. New statutes specifically directed toward computer crime have provided new, but largely untested, tools for the prosecutor's use. These statutes reflect the specific criminal events that have occurred as computer use has increased. The tests will come as cases are prosecuted and convictions obtained.

Although current Minnesota law specifically addresses computer-related crime, there are still a number of issues pertaining to this topic which need to be examined:

1. Many computer theft cases involve a number of small thefts committed over a period of time. In order to cover the aggregation of computer thefts, it is necessary to either attach an aggregation provision to the computer crime statute or to make a reference to the computer crime law in the aggregation section of the theft statute.

   The aggregation provision contained in the theft statute states that in all cases where 1) the value of property or services stolen is $150 or less, 2) imprisonment is not more than 90 days, or 3) payment of a fine is not more than $500, the value of the money or property received by the defendant in any six month period may be aggregated and the defendant charged accordingly. Therefore, an individual who commits a number of small theft offenses within a six month period may be charged with a felony and sentenced according to the sentencing guidelines. This provision, however, applies specifically to the theft statute. The computer crime statute now in effect does not have an aggregation provision.

2. It can take an exceedingly long time to detect and investigate a computer-related crime. It is therefore necessary to amend the statute of limitations on white collar crimes--particularly computer-related crimes--to allow prosecution for three years from the date of detection,

not to exceed five years from the date of occurrence of the offense. The federal statute of limitations provides for a five-year limit from the date of occurrence.

3. There is a need to further examine the civil liability aspect of computer-related crime. Increased civil liability may prove to be the most effective means of handling computer crimes; at the same time, it may be the most difficult to define and the most difficult to obtain in the legal system.

4. The subcommittee recognizes that computers are related to the field of communications technology, and that changes in other areas (such as cable systems and microwave telecommunications) will have a direct impact on the use of computers and the incidence of computer crime.

   The subcommittee feels that there is a need for laws governing cable communications security. Cable systems are going to be major carriers of data and the possibility of abuse of cable systems is significant. The state should examine the process used in developing the computer security legislation and follow similar procedures in developing laws governing the security of cable systems. In addition, security control mechanisms for cable systems need to be developed and put into use.

5. A major concern of those involved in computer security is the continuing emergence of networks of computer users who communicate via "electronic bulletin boards." While this report does not specifically focus on cable and microwave technologies, it is not intended to exclude the problems associated with networks. A bill has been introduced in the Wisconsin legislature that would control the information put on electronic bulletin boards. The state of Minnesota should monitor this legislation and further examine the issue.

   Associated with this issue, is a concern about the numerous ways of accessing computer systems and computer networks and the problems of controlling that access. Subcommittee members agree that further study is needed to determine whether the current law adequately addresses the definition of access as well as the problem of "attempted" access. In addition, there is a need to examine the possibility of modifying the statute to address "unauthorized use" of a computer.

6. Venue basically is the legal issue of the place where a crime has taken place and, thus, where it should be prosecuted. It is a very complex problem when computer crime is considered. The triggering events are actually the activation of electronic "switches" which can be done from outside the city, state, or even nation in which the receiving computer is located. Once triggered, the computer can transfer money or its program again to yet another state. The signals can even travel through space by satellite.

An example of a computer crime case that crossed many jurisdictional lines occurred in 1978. In that case, an individual manipulated the Federal Reserve System's electronic funds transfer network to initiate a $10.2 million transfer from Security Pacific Bank in California to a bank in Switzerland.

The subcommittee recommends that a statute be adopted defining all of the following locales as appropriate venues for the prosecution of the computer criminal:

a. The place from which the triggering signals were issued.

b. The place at which the recipient computer is located.

c. The location of the institution where the loss of benefit is sustained.

d. The place at which the ultimate benefits, funds or services are received.

7. A conviction for a computer crime appears on the Minnesota sentencing guidelines grid in the same place as theft. Theft crimes appear on the grid on both the third and fourth levels, depending on the dollar amount of the theft. If a conviction is for an offense with an amount between $150 and $2,500, it is a level III offense. If the amount is greater than $2,500, it would be a level IV offense.

   Since most individuals convicted of computer crimes are first time offenders with no criminal history, they do not serve prison time if the sentencing guidelines are applied. Therefore, if a prosecutor feels imprisonment is warranted, it is necessary to seek departure from the guidelines. Under certain circumstances, a judge may depart from the established sentence and stay or impose any sentence authorized by law. A list of factors that may be used as a basis for this departure has been developed by the Minnesota Sentencing Guidelines Commission.

8. Increased awareness of the law pertaining to the misuse of computers is needed. If the law is to be an effective deterrent, it must be publicized.

9. There is a need for a periodic review of the state's computer crime statute. Because computer technology changes so rapidly, new problem areas may arise which are not covered under this law. In addition, as the law is tested, issues will arise which require clarification or further study.

   The subcommittee feels that the following aspects of the Minnesota Law on Computer Damage and Computer Theft (see Appendix) need to be examined:

   a. There is a need to clarify "...intent to permanently deprive..." as stated in Section 609.89, Subdivision 1(b) of the law. It is not clear how one can prove that a party intended to take something "permanently."

b. There is a need for an interpretation of "...takes, transfers, conceals or retains possession of any computer, computer system or any computer software or data contained in a computer, computer system or computer network as stated in Section 609.89, Subdivision 1(b) of the law. This sentence implies that the data must be contained in the computer, therefore ruling out all of the manuals, procedures, and software external to the computer.

c. There is a need to incorporate the development and preparation of materials into Section 609.87, Subdivision 10 which defines "loss."

PREVENTION AND CONTROL

Prevention of computer misuse is the joint responsibility of users, computer hardware and software suppliers, service vendors and the law enforcement community.

There is a perception by some computer users that, because misuse has not been uncovered, it does not exist. And when it is discovered, overreaction frequently occurs. Other mistaken beliefs include thinking that someone else is taking care of security; existing precautions are adequate; or that the subject may safely be delegated to suppliers or the user's technical staff. These beliefs reflect a lack of understanding. There is, indeed, cause for concern and action in the protection of computer equipment, processes and information.

Schools are beginning to address the appropriate use of computers as part of their computer literacy curriculum. For example, the Bloomington School District has been awarded funding for a special pilot grant project to develop materials and instructional modes that address computer ethics and user responsibility. The subcommittee recommends that schools incorporate into their computer literacy curriculum ways of heightening awareness of the legal and personal ramifications of computer misuse. School personnel should also share curriculum information on this topic with other schools through existing networks in an attempt to sensitize the educational system to the need.

Educational curricula and employer-supplied education vary, but the computer technician is usually not formally educated in security principles. Technical priorities are efficiency and technical accomplishment. Employees and their managers may feel that security requires extra work that impairs their efficiency. As a result, they may take shortcuts that undermine the security of the computer system.

Precise statistics on frequency and resulting losses from computer misuse are not available. There is a need to properly collect and present data in this area. Understanding risks and properly managing for them is also necessary. If security controls are put into place only as a reaction to a loss, they may not be as effective.

Responsibility for computer security should not be delegated to a single specialized group. Such specialized groups as security, audit, and computer operations may provide assistance, but only the managers of an organization can know and ensure that controls are properly applied. Management remains responsible for business continuity and the assets--people, data, software and hardware--of the company. Management must, therefore, supply the driving force in addressing security concerns.

There is a need for specific organizational policies and procedures related to the use of computers and computer misuse. For example, responsibility for reporting computer misuse should be clearly defined; there should be a policy regarding taking software home to work on; and there should be guidelines for passwords. In addition, there is a need for management to reaffirm on a regular basis that they believe in and adhere to ethical business practices, and they expect their employees to do likewise.

Management control of the operation of in-house computer systems needs to be greater. There is a need to upgrade awareness of the importance of internal computer control systems. Management must also be better educated about the vulnerability of their computer systems and be made aware of the safeguard options available. And when internal controls are in place, there is a need to regularly reexamine whether controls are adequate.

Managers need to become more aware of, and involved in, the day-to-day operation of computer systems. A questioning attitude about how computer systems and controls are functioning should exist.

SECURITY EDUCATION

Increased awareness of security concerns with respect to computer systems is needed. Two kinds of security must be taken into consideration: the actual physical security of the computer hardware, and protection of the data contained in the computer by encoding data and limiting access to it. Security technology or mechanisms may be available, but people have to be made aware of the vulnerability of their computer systems and of the protections available. It is uncommon for manufacturers to disclose the vulnerability of their systems when they are trying to sell their goods but they should be encouraged to point out security risks.

Law enforcement agencies can play a key role in the security education process. Through community relations activities, public forums and the use of brochures and pamphlets, such agencies can make those people using computer systems aware of the types of crimes that are being committed and what to look for.

Law enforcement agencies can also assist businesses by conducting surveys of the business premises. Such surveys can be useful in determining an effective means of controlling physical access to a computer system. This is particularly important for small business owners since they may have very limited knowledge of the vulnerability of the computer system.

Again, there is a need to get the computer security problem out in the open where it can be examined--and managed. By getting people to conduct a risk analysis or security impact study before putting in new computer systems, better controls could be put into place. Checklists should be made available, either from law enforcement agencies or from public accounting and private consulting firms, to assist businesses in conducting security analyses. The availability of these checklists should be widely advertised so that small users in particular would be able to obtain them.

It is recommended that security education activity be increased with emphasis on prevention and detection techniques. The objective should be to move from a reactive to a proactive computer security environment. It is especially important that those people who use computer systems on a regular basis receive training to make them aware of computer security issues. It is also important that they be made aware of internal policies and procedures related to computer misuse.

COMPUTER HARDWARE AND SOFTWARE MANUFACTURING

Many security safeguards are available as user options from suppliers or manufacturers. Implementation is left to the user's discretion. Password systems and internal audit trails are common security controls.

The computer industry recognizes that while there are excellent security mechanisms, most computer users have not taken full advantage of them. For example, data encryption (a method of disguising data) is available from approximately twenty-five manufacturers, but is seldom used. Computer hardware and software systems are designed to take advantage of electronic speed. Efficiency and productivity are the essential underlying theme. Security features expend computer resources and can impair efficiency since they use memory space and can slow down processing. They also raise product cost. Almost all computers are designed with multiple security features. Additional safeguards can be developed by the user or provided as required by the supplier. The committee finds that security is more of an administrative and financial challenge than a technological one.

The computer industry has evolved quickly and has grown rapidly in response to market demand. The industry's firms range from single-party enterprises to large corporations. The market demand for security also is growing steadily. With demand growing, security features provide a competitive marketing advantage and an incentive for suppliers to make additional investments in security features.

Protection of computer networks and network interconnections is of prime importance. There are currently a number of techniques available for increasing the security of networks including use of dedicated lines, encryption, and different levels of password security, but new and more effective methods of protection need to be developed.

DETECTION AND REPORTING

Cases of computer misuse historically have been discovered by accident. There has been little or no proactive security detection. Industry detection tools exist, but these require specific individual assignments, accountability, and ongoing dedication of resources. Detection responsibility needs to be specifically assigned.

Even when possible breaches of computer security are noted by the computer system they are not always reported or fully investigated. Many computers maintain an audit trail or an access record, but breaches from standard practice are often not passed on or investigated. One kind of proactive detection could be review of such logs on a regular basis. Detection is a particularly difficult challenge for small businesses with limited resources.

Detection programs can also serve as a deterrent. Management commitment to security shown through dedication of detection resources with the resulting increased chance of discovery, will help prevent misuse.

Computer misuse and computer crime are often not reported to management, law enforcement agencies or insurers. The risk of incurring additional loss and possible damage to credibility are major factors. Businesses are also reluctant to reveal employee misconduct due to internal personnel policies and procedures protecting the privacy of information on employees. In addition, some companies may believe that the law enforcement community is not adequately trained in the handling of misuses of computer systems.

Economic and/or external factors often determine if reporting will occur. For example, a company that is planning a stock offer or is about to be acquired certainly will not reveal their computer system has been breached.

The subcommittee feels all victims of computer crime should be encouraged to report their losses to law enforcement agencies. In addition, insurance companies should be encouraged to include a requirement that insured victims report any losses to a law enforcement agency in policies covering computer systems.

The subcommittee feels that there are a number of problems associated with non-reporting of computer crimes. These include:

- Failure to report computer misuse may encourage its proliferation. If the chances of being punished are minimal, there is greater likelihood that misuse will occur.

- If employees see that such crimes are not being reported, it may erode their confidence in the company. This presents a challenge to the integrity of the American business community.

- Employees who have misused a computer system in one business can go to other companies and commit similar offenses.

- Businesses, especially small businesses, may be forced to increase product prices in order to absorb the losses sustained through computer crimes.

- When offenses are not reported, the extent of the problem of computer crime is unknown.

- Shareholders may be unaware of possible difficulties within a company.

The subcommittee is concerned that the public be informed of computer misuse. At the same time, the release of too much information may result in further damages to companies. To balance these concerns, the following points need to be examined.

- Mechanisms available to protect the anonymity of the company or industry reporting.

- Incentives and penalties for reporting or non-reporting.

- Computer crime reporting versus reporting of traditional crimes.

- The reason for reporting the misuse--to provide information about the problem or to pursue prosecution of the offender.

- Effective ways of encouraging voluntary reporting.

- Ways of educating the public about where to report computer misuses.

- The possibility of surveying private industry on a one-time or periodic basis to determine the extent of computer misuse.

INVESTIGATIVE COOPERATION BETWEEN INDUSTRY AND LAW ENFORCEMENT AGENCIES

Computer crimes cannot be effectively investigated without a cooperative working relationship between law enforcement agencies and private industry.

The law enforcement community is best able to understand the requirements for prosecution. They are also well equipped to deal with external transactions and proceeds from a crime. It is not practical, however, for all law enforcement agencies to have sufficient staff expertise to understand all the technical aspects of a given computer crime. Specialized technical training loses value to law enforcement investigators unless these officers have regular involvement with cases requiring technical expertise.

It is necessary, therefore, for law enforcement agencies to be able to identify and mobilize sources of expertise in this area to be tapped as needed. It is also important for agencies to develop ongoing working relationships with key technical advisors (EDP auditors, computer security specialists and experienced investigators from other jurisdictions) who can provide assistance with computer crime investigations. These resources have specialized knowledge, training and experience which can strengthen the investigative process.

It is also important that cooperation and sharing of knowledge between law enforcement agencies be increased. Computer crime cases most often will exceed the technical expertise of local law enforcement agencies. Therefore, it is essential that these agencies know where law enforcement personnel are available who are specially trained in this area.

The subcommittee has concluded that initiatives to encourage joint cooperative working relationships are needed. It is important to examine ways of increasing communication and sharing information and resources between private industry and law enforcement agencies. Areas where a cooperative working relationship is needed include:

- There is a need for technical assistance in drawing up search warrants so that investigating officers have accurate information about which items to look for.

- When a search warrant is executed, it may be necessary to have someone with technical expertise accompany the investigating officers to ensure that the computer evidence (such as computer discs) can be found and stored properly. If there are a number of computers and software products, the expert can determine which articles are to be seized. The use of citizens acting in conjunction with law enforcement agencies in this role requires further examination since there are certain liability questions which may arise.

- There is a need for equipment and technical expertise to help the investigators understand the evidence seized.

- There is a need to identify and share specialized computer security expertise.

- There is a need to identify training needs and share training resources.

THE COMPUTER AS AN INVESTIGATIVE TOOL

In the course of studying the topic of computer crime, the subcommittee has found that the computer can also serve as a valuable resource for law enforcement personnel to use in the course of their investigations. Some examples of the ways that computers can be used include:

- Analysis of case data.

- Retrieval of case information.

- Tracking the method of operation of a particular case.

- Tracking crime trends.

Several law enforcement agencies in the Metropolitan Area currently use computer systems in the course of their work. There is a need, however, for further training on computer system capability and availability for investigative work. There is also a need for greater cooperation in the use of computer systems between local and state law enforcement agencies.

It is hoped that as use of the computer as an investigative resource increases law enforcement personnel will become more familiar with computer technology. This, in turn, will increase their awareness of computer problems and improve their ability to address computer crime.

TRAINING OF LAW ENFORCEMENT PERSONNEL

Specialized training on the topic of computer crime should be provided to those law enforcement personnel who are involved in the investigation of white collar crimes. This training should address the problem of computer security, the general terminology, the current law (as it relates to search and seizure specifically), and some case studies. Information on where individuals with more expertise are available should also be included. Perhaps one of the most important points to be addressed in this training is the necessity for calling in individuals with specialized computer expertise to assist in the handling of the more technical aspects of a computer crime case.

These training activities perhaps could be offered and paid for through a coordinated effort of the state Bureau of Criminal Apprehension (BCA), the FBI and private industry. Such training could also be provided as part of continuing education programs for law enforcement personnel.

It also would be beneficial if private industry would allow the public law enforcement sector to participate in, or to observe, some of their internal training and coursework on computers.

The FBI has an extensive training program on computer crime investigation, but this training is available to only a limited number of law enforcement personnel. The state of the art is changing rapidly so it would not be efficient to provide highly specialized training for all law enforcement personnel. It is felt that it would be best to have a few highly trained law enforcement specialists in the Metropolitan Area and to rely on outside consultant resources to meet additional special needs. Those individuals who have participated in the FBI training program could serve as resources to other law enforcement investigators and prosecutors.

PRIVATE SECURITY

Greater efforts need to be made to increase the role of private security in controlling computer crime or misuse. Corporate security departments are in a key position to understand and deal with internal situations.

In most cases, private security has not been heavily involved with internal use of computers. Many large businesses have two levels of security: staff who are assigned responsibility for general security of the physical environment; and staff who are assigned responsibility for specific security

of the computer system. The growing number of computers, computerized processes, computerized data and computer users mandates more involvement and more communication between all personnel involved in the security function. Increased internal coordination should be encouraged, especially when security responsibilities are divided between different departments.

Security directors need to amplify the need for concern, act as a catalyst in bringing concerned parties together, and develop safeguard policies and practices.

Regardless of whether security is internal or handled through a contractual arrangement with an outside firm, the reporting system should be carefully thought out. It is important that the findings and recommendations of security personnel be given serious consideration. Therefore, it is critical that they report to someone in top management who is in a position to implement change and take other appropriate action as needed. It is also important that security personnel report to someone independent of an area under investigation, since there is a possibility that management in that area may try to cover up inadequacies in their system.

ROLE OF THE INSURANCE INDUSTRY

Insurers have provided fidelity insurance coverages to employers for years. Typically, fidelity insurance protects the firm from loss of tangible property caused by theft by employees, whether or not a computer was used in the crime. Fidelity underwriters now are recognizing that the computer creates significant potential risk, and are modifying their coverages and developing new insurance programs. This is being done to recognize the computer theft exposure and refine underwriting approaches to better relate to these new problems. Some of these new coverages also cover theft by outsiders who access an on-line system.

As insurance companies begin to categorize computer-related theft and claims activity increases, they will develop data on losses. This data could prove valuable to those particular insurers writing the coverage, and in a larger sense to the industry, as it coordinates this information. Computer theft loss activity--as it increases--will require underwriters to focus on the key issues of loss prevention and control. Insurers will increasingly require effective management controls as a prerequisite of providing computer theft coverage. As this process evolves, the insurance industry should take an increasingly important role in management of computer theft risk.

Insurers will need to focus on an effective means of sharing information resulting from losses with other insurance companies, law enforcement agencies, the computer industry and computer users. This effort can be a part of a combined thrust to increase awareness of risks associated with greater dependency on computers. The various sectors should begin working together now.

SPECIAL NEEDS OF SMALL BUSINESSES AND FIRST-TIME COMPUTER USERS

Businesses with fewer than 50 employees create the most new jobs, and take large risks. At the same time, these businesses have fewer resources to apply to computer security and are vulnerable to a single failure, misuse or fraud.

Small businesses and first-time computer users have three principal computer security needs: 1) education in security awareness, 2) low-cost security features which can be easily applied, 3) computer security expertise which can be made available quickly.

Processes to meet these needs should be developed.

NEED FOR ONGOING COORDINATION AND COOPERATION

Neither government nor private industry alone can afford to develop and maintain expertise necessary to adequately cope with the full range of computer security issues. Cooperative assistance programs are needed to address these issues on an ongoing basis. Such programs should increase practical cooperation between the public, law enforcement and private technology sectors, as well as the insurance industry and the legal and academic communities. In addition, such programs should provide opportunities for voluntary consultation on matters pertaining to computer misuse and computer security.

Networks which deal with white collar crime issues are currently in existence in the Metropolitan Area. One example of such a network is the inter-agency economic crime unit which meets monthly at the state Bureau of Criminal Apprehension. This particular network enables law enforcement personnel who have an interest and working involvement with white collar crime issues to come together to share information and experiences. It is suggested that a subcommittee be established under this white collar crime unit to focus on the specific problems associated with computer abuse and computer security. Such a subcommittee should be responsible for keeping informed about new developments pertaining to this topic and for knowing what resources are available in this area. It could also serve as a resource pool to provide information and assistance to those requesting it.

Other networks whose members are involved in addressing computer crime and computer security issues (such as the Bar Association, trade associations, auditors groups and academic groups) should set up similar subcommittees to keep their membership current on activities pertaining to this topic.

ROLE OF THE METROPOLITAN COUNCIL

It is recommended that an ongoing computer security task force be established. This task force should be responsible for the following:

1. Coordinating the development of resource networks for the exchange of information on computer security issues.

2. Identifying public agency and private sector efforts to address computer security issues in the Metropolitan Area. Compiling a list of available resources.

3. Serving as a clearinghouse for information on computer security issues as well as the availability of experts in this area.

4. Assessing the nature and extent of the problem of computer misuse in the Twin Cities Metropolitan Area.

5. Identifying upcoming issues pertaining to computer misuse and computer security. Serving as a focus for discussion on these issues.

6. Working to carry out the recommendations contained in this report.

APPENDIX

MINNESOTA LAW ON COMPUTER DAMAGE AND COMPUTER THEFT
(Laws 1982, Chapter 534)

609.87 COMPUTER CRIME: DEFINITIONS.

Subdivision 1. APPLICABILITY. For purposes of sections 609.87, 609.88, and 609.89 the terms defined in this section have the meanings given them.

Subdivision 2. ACCESS. "Access" means to instruct, communicate with, store data in, or retrieve data from a computer, computer system, or computer network.

Subdivision 3. COMPUTER. "Computer" means an electronic device which performs logical, arithmetic and memory functions by the manipulations of signals, including but not limited to electronic or magnetic impulses.

Subdivision 4. COMPUTER SYSTEM. "Computer system" means related, connected or unconnected, computers and peripheral equipment.

Subdivision 5. COMPUTER NETWORK. "Computer network" means the interconnection of a communication system with a computer through a remote terminal, or with two or more interconnected computers or computer systems.

Subdivision 6. PROPERTY. "Property" includes, but is not limited to, electronically processed or produced data and information contained in a computer or computer software in either machine or human readable form.

Subdivision 7. SERVICES. "Services" includes but is not limited to, computer time, data processing, and storage functions.

Subdivision 8. COMPUTER PROGRAM. "Computer program" means an instruction or statement or a series of instructions or statements in a form acceptable to a computer, which directs the functioning of a computer system in a manner designed to provide appropriate products from the computer.

Subdivision 9. COMPUTER SOFTWARE. "Computer software" means a computer program or procedures, or associated documentation concerned with the operations of a computer.

Subdivision 10. LOSS. "Loss" means the greatest of the following:

(a) the retail market value of the property or services involved;

(b) the reasonable repair or replacement cost, whichever is less; or

(c) the reasonable value of the damage created by the unavailability or lack of utility of the property or services involved until repair or replacement can be effected.

609.88 COMPUTER DAMAGE.

Subdivision 1. ACTS. Whoever does any of the following is guilty of computer damage and may be sentenced as provided in subdivision 2:

(a) Intentionally and without authorization damages or destroys any computer, computer system, computer network, computer software, or any other property specifically defined in 609.87, subdivision 6; or

(b) Intentionally and without authorization and with intent to injure or defraud alters any computer, computer system, computer network, computer software, or any other property specifically defined in 609.87, subdivision 6.

Subdivision 2. PENALTY. Whoever commits computer damage may be sentenced as follows:

(a) To imprisonment for not more than ten years or to payment of a fine of not more than $50,000, or both, if the damage, destruction or alteration results in a loss in excess of $2,500, to the owner, his agent, or lessee;

(b) To imprisonment for not more than five years or to payment of a fine of not more than $5,000, or both, if the damage, destruction or alteration results in a loss of more than $500, but not more than $2,500 to the owner, his agent or lessee; or

(c) In all other cases to imprisonment for not more than 90 days or to payment of a fine of not more than $500, or both.

609.89 COMPUTER THEFT.

Subdivision 1. ACTS. Whoever does any of the following is guilty of computer theft and may be sentenced as provided in subdivision 2:

(a) Intentionally and without authorization or claim of right accesses or causes to be accessed any computer, computer system, computer network or any part thereof for the purpose of obtaining services or property; or

(b) Intentionally and without claim of right, and with intent to permanently deprive the owner of possession, takes, transfers, conceals or retains possession of any computer, computer system, or any computer software or data contained in a computer, computer system, or computer network.

Subdivision 2. PENALTY. Anyone who commits computer theft may be sentenced as follows:

(a) To imprisonment for not more than ten years or to payment of a fine of not more than $50,000, or both, if the loss to the owner, his agent, or lessee is in excess of $2,500; or

(b) To imprisonment for not more than five years or to payment of a fine of not more than $5,000, or both, if the loss to the owner, his agent, or lessee is more than $500 but not more than $2,500; or

(c) In all other cases to imprisonment for not more than 90 days or to payment of a fine of not more than $500, or both.

EFFECTIVE DATE.

This act is effective August 1, 1982 and applies to all crimes committed on or after that date.

DM009A