COMPUTER CRIME

Criminal Justice

National Criminal Justice Information and Statistics Service
Law Enforcement Assistance Administration
U.S. Department of Justice

U.S. DEPARTMENT OF JUSTICE
Law Enforcement Assistance Administration

Henry S. Dogin, Administrator

Homer F. Broome, Jr., Deputy
Administrator for Administration

Benjamin H. Renshaw, Acting
Assistant Administrator
National Criminal Justice Infomation
and Statistics Service

Carol G. Kaplan
Director, Privacy and Security Staff

COMPUTER CRIME

Criminal Justice

National Criminal Justice Information and Statistics Service
Law Enforcement Assistance Administration
U.S. Department of Justice

This document was prepared for the National Criminal Justice Information and Statistics Service of the Law Enforcement Assistance Administration, U.S. Department of Justice, under Grant No. 78-SS-AX-0031 awarded to SRI International. Points of view and opinions stated herein are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice or of SRI International.

INTRODUCTION

Business executives must deal with business, economic, and white-collar crime either as victims, observers, or witnesses of this growing, major problem. According to the U.S. National Chamber of Commerce, this kind of crime, called fraud, theft, larceny, embezzlement, extortion, conspiracy, bribery, sabotage, and industrial espionage, costs up to $40 billion per year in losses.

Today, a new form of crime, called computer-related crime, is resulting in new, even more serious problems as computers proliferate and are being used in high-risk environments and activities where the traditional crimes have occurred. While the use of computers is making business safer from crime in many ways, the computer has spawned criminals in new occupations, and new criminal environments, crime methods, targets of crime, timing of criminal acts, and geographic boundaries for perpetration of criminal acts.

Crime has traditionally occurred in environments of various manual activities. Now some crimes occur inside computers in the environment of rooms with raised flooring, lowered ceilings, large grey boxes, flashing lights, moving tapes, and the hum of air-conditioning motors. Criminals may now be found among computer programmers, computer operators, magnetic tape librarians, and electronic engineers.

The potential victims include all organizations and persons who use, or are affected by, computer and data communication systems.

Many other aspects of computer-related crime also are new and must be considered in dealing with computer abuse. Computer-related crimes have generated a new jargon identifying automated criminal methods, such as data diddling (changing input data), Trojan horses (putting secret instructions in computer programs), and salami techniques (taking small amounts from a large number of accounts).

The forms of many of the targets of computer-related crime are also new. Electronic money as well as paper money and plastic money (credit cards) now represent assets subject to theft. Money, in the form of electronic signals and magnetic patterns, is stored and processed in computers and transmitted over telephone lines. Money is debited from and credited to accounts inside computers. In fact, the computer is rapidly becoming the account book and vault of the business community. Many other physical assets, including inventories of products in warehouses and of materials leaving or entering factories, are represented by documents of record inside computer systems.

The duration and timing of some computer-related crimes is also different. Traditionally, criminal acts were measured in minutes, hours, days, weeks, months, and years. Today some crimes are being perpetrated in less than 0.003 of a second (3 milliseconds). Thus, automated crime must be considered in terms of a new time scale because of the speed of the execution of instructions by computers.

Geographic constraints no longer inhibit crime either. A telephone with a computer terminal attached to it in one part of the world might be used to engage in a crime in an on-line computer system in any other part of the world.

Organizations that use computers generally lose far more from accidental loss caused by errors and omissions than that from intentionally caused losses. Therefore, it may seem reasonable to concentrate on carelessness rather than crime forgetting that one opens the door to the other. There are important reasons why we should give a high priority to the prevention, detection, and deterrents of computer-related crime.

We have been battling errors and omissions in the computer field since its beginning. There are few unsolved problems in dealing with these single, isolated acts that usually involve only one person in a job location where intense detailed human activity occurs. Minimum skills of the perpetrators of errors and omissions are at issue. The losses are limited, there is no premeditation, and reporting of losses is a commonly accepted practice. Such is not the case with intentionally caused losses.

Safeguards against accidental loss generally are not effective against intentionally caused loss. In contrast, safeguards applied against intentional acts are generally effective against a wide range of accidental loss. But many unsolved problems remain in dealing with intentionally caused losses. There are no effective safeguards against some of the sophisticated, computer-related crime methods which have succeeded.

Intentional acts in contrast to accidental acts are more likely to be highly complex, frequently involve collusion, occur in obscure areas, involve large undetected losses, and use the maximum skills of the perpetrator. A relatively low incidence of recognized intentional acts makes security expenditures difficult to justify even though individual losses can be massive. These arguments all support the need for addressing the more difficult of the two problems with the greater amount of security resources.

One of the most important and effective actions that victims of computer-related crime can take is the reporting of all suspected incidents to the law enforcement authorities. This not only is a strong deterrent to computer-related crime, but also provides factual information needed to develop the safeguards that may protect other potential victims from suffering similar losses.

DEFINING COMPUTER-RELATED CRIME

Many believe that computer-related crimes consist of acts inside computers. This narrow definition has been broadened as the use of computers in more business functions proceeds at an increasing pace. From the business executive's point of view, all intentionally caused losses associated in any way with the use of computers must be effectively reduced. Hence, a comprehensive definition of computer-related crime is essential to deal effectively with crime in whatever ways it is associated with computer technology.

One definition of computer-related crime terms it a form of white-collar crime committed inside a computer system. Another defines it as the use of a computer as the instrument of a business crime. An example of the former is a computer programmer in a bank making unauthorized changes to a computer program causing a computer to transfer funds from inactive accounts into a favored account and then covertly but legitimately withdrawing the funds. An application of the latter definition of crime occurred when the management of an insurance company used the company computer to create 64,000 fake insurance policies for resale to other insurance companies. These are only two of the many aspects of computer-related crime. Clearly, a broader definition of computer-related crime is needed.

Computer-related crime is basically any illegal act in which knowledge of computer technology plays a role in its perpetration. This same technical knowledge is needed for successful prosecution. Crimes may involve computers in active roles and passively when evidence of the acts is in computer-stored form. It even includes violent crime when computers or their content are destroyed or when human life and well-being are jeopardized because they are dependent on sensitive processes which are controlled by computer.

Computers have been found in four roles in crime:

- o Objects: Cases include destruction, modification, taking, or unauthorized use of computers or data and programs contained in them or involve supportive facilities that are required for operation, such as air-conditioning equipment and electrical power.

- o Subjects: A computer can be the site of a crime or the source of unique forms and kinds of assets such as electronic money.

- Instruments: Some types of crime are complex enough to require the use of a computer as a tool or instrument. A computer can be used actively, such as in automatically scanning telephone codes to make unauthorized use of a telephone system. It could also be used passively to simulate a general ledger accounting system in the planning and control of a continuing financial embezzlement.

- Symbols: A computer can be used as a symbol for intimidation or deception. This could involve the false advertising of non-existent services of a computer as offered by dating bureaus.

All known and reported cases of computer-related crime involve one or more of these four roles. As the computer increasingly plays the role of the vault and processor of business assets and business records, it becomes more imperative to ensure the safety of organizations through adequate security and prompt reporting of incidents to the proper authorities.

MANAGEMENT ACTION AGAINST COMPUTER-RELATED CRIME

A computer security program must be developed using technical methods and other safeguards. Computer security requires deterrence, prevention, detection, recovery, and correction methods that use operational, procedural, personnel and physical access controls. Most important are security policies, and procedures established and supported by management. Security also includes the prompt reporting of loss incidents to the proper authorities.

The following list of management actions is recommended for use in developing a security program:

o Assign management responsibility for computer security. Security is a line management responsibility. Each line manager is responsible for the security, integrity, and safety of the activities within his area.

  - Computer security coordinators or ad inistrators should be establisℎed to assist line management in performing security responsibilities. This function is best placed in the data processing organization or in the security office of the organization.

  - The audit function must also be adequately prepared to audit in computer environments by establishing an electronic data processing (EDP) audit specialty and capability.

- o Perform a complete security review periodically and at key times. Security reviews can be conducted by specially appointed task forces under the direction of the computer security manager or administrator. The auditors should also participate in this activity. A computer security review consists of the following steps:

  - Assets identification.

  - Potential threats recognition.

  - Vulnerability analysis based on current safeguards.

  - Risk analysis to rank or measure the severity of vulnerabilities.

  - Identification of safeguards for upgrading security.

  - Selection and implementation of safeguards.

- o Perform limited update security reviews in environments where significant changes occur.

- o Ensure adequacy of controls and auditability in new and modified applications, computer equipment, and computer programs.

- Ensure the trustworthiness of employees consistent with their positions of trust through careful hiring and personnel practices.
- Require annual security briefings of all such employees.
- Establish and periodically test disaster recovery plans.
- Establish and perform upward reporting to management of all losses and actions taken.
- Establish procedures and responsibility for the reporting of suspected criminal acts to the proper authorities.

An aid for the safe use of computer technology is the establishment of principles of business conduct, standards of computer-related conduct, and appropriate sanctions against the violation of these codes. Examples of codes can be obtained from large business organizations.

LAWS AGAINST COMPUTER-RELATED CRIME

Federal and state criminal laws are rapidly being changed to deal with the changing nature of crimes associated with computers. A number of states already have explicit criminal laws to deal with computer-related crime, and legislation in other states and at the federal level is pending. Victims of alleged computer-related crimes can be confident that adequate criminal laws exist to deal with any problems they may experience. Prosecutors generally agree that they have been able to successfully prosecute computer-related crime in all acknowledged cases.

Many existing federal criminal laws are applicable to computer-related crime. For example, applicable federal laws include the new Foreign Corrupt Practices Act, the Privacy Protection Act of 1974, mail and wire fraud statutes, and many others. In addition, existing state fraud, theft, larceny and conspiracy laws as well as new explicit computer-related crime laws may be applicable and must be considered.

WHY SUSPECTED COMPUTER-RELATED CRIME SHOULD BE REPORTED

It is a civic and ethical duty to report suspected crime for prosecution. Moreover, it is only fair to society that computer-related crime perpetrators be restrained from doing further harmful acts and be punished for past misdeeds. This can be done properly through successful prosecutions and convictions. In addition, timely reporting of suspected crimes is important to increase the likelihood of apprehension of suspected perpetrators and recovery of losses. For example, when claims are filed to recover losses, fidelity bonding insurance companies require that the loss has been reported to authorities.

Swift and certain prosecution and the application of just sanctions against convicted perpetrators represent strong deterrents to others who may attempt crime. This is particularly important in the computer area where little experience and precedence have been established. Computer technologists must be shown as quickly as possible that unauthorized acts they might perform in computer environments can be serious crimes. This will discourage those who might rationalize that such acts are not very serious because no one has ever done them before: it's done to a computer and not to people, and the methods used to commit the act have not been identified as crimes.

REPORTING A SUSPECTED CRIME

It is advisable for an organization that could be the possible victim of computer-related crime to establish early liaison with particular members of the local criminal justice community who deal with this problem and welcome this kind of contact. These contacts include the police department (sheriff's office in the case of unincorporated areas)--where suspected crimes usually are reported--local and federal prosecutors, and the Federal Bureau of Investigation (FBI). Regulated financial institutions, such as banks, are required by law and regulation to report suspected crimes in specific ways that are well-known to them. Federal or local jurisdiction of an incident can be difficult for a victim to determine.

Therefore, this should be left to whatever authorities receive the complaints.

Making such contacts before a computer-related criminal act is committed also serves other purposes. First, it helps to prepare potential victims in knowing what records they need and procedures to follow in the event a crime occurs. Second, it identifies the needs of local authorities to deal with the complex technology often associated with computer-related crime. Finally, this mutual understanding can aid in loss recovery and can significantly abet investigation and prosecution of computer-related crime. This action alone does not obligate the victim, however, to report a suspected crime.

Steps to be taken to report a suspected computer-related crime are as follows: Make a report to the local law enforcement agency. Most computer-related crime probably will be reported as theft, and the specialist in major fraud or larceny will be assigned to the case. Report the incident to the district attorney's office. This will alert the prosecutors who will ultimately handle the case. This office also is a good source of guidance in how to proceed. Report to the local FBI office if there is any question that there may be a federal jurisdiction for the case.

It is important to inform each contacted organization about contacts made to any other agencies so as to enable them to coordinate their efforts.

When a suspected crime is reported to the authorities, however, it should be done on the basis of a full commitment to support the prosecution of the alleged crime. Obtaining the full and continuing support of the victim is critical to the prosecutor's decision whether to commit resources to the investigation and prosecution of the offense.

ESTABLISHING POLICY ON REPORTING SUSPECTED CRIME

An organization should establish and document a policy for guidance in handling a suspected computer-related crime. All employees should be expected to report possible offenses or suspicious activity. In many organizations, the security or protection department, with the authorization of top management, screens or reports the suspected act.

It is important that as few people as necessary know about or participate in the process of handling these situations. The policy should make provisions to protect the rights of all parties and to avoid the dangers of undesirable publicity, any unfairness to the parties to the suspected crime, and the possibility of legal action taken against the victim by such parties.

If there is any indication that information of an alleged or suspected crime might be made public, it is important that the policy stipulate the activity of the public relations or public information officer within an organization. In that this is always a real possibility, an organization should designate a single spokesman and notify all other parties related to the incident of this action. Press releases should be carefully planned and coordinated with all parties to the investigation.

HANDLING EVIDENCE AND INVESTIGATION

It may be difficult to determine what constitutes evidence of a suspected crime. Guidance from a district attorney's office and from private legal counsel is particularly valuable in this matter.

All actions in an investigation must be carefully documented. Case reporting and investigation forms are helpful. A useful document, "Computer Crime; Criminal Justice Resource Manual", prepared for the Law Enforcement Assistance Administration (LEAA) of the U.S. Department of Justice, is available from the U.S. Government Printing Office, Washington, D.C.

Care should also be taken in the collection and preservation of evidence in the form of computer media such as magnetic tapes, magnetic disks, computer hardware components, computer programs, and related documentation. Original items should be safeguarded in appropriate environments for their preservation, and copies of them should be made or obtained if they are needed for continued operational purposes.

There is a danger of losing evidence in some types of computer-related crime; the computer provides great leverage in processing, modifying, or erasing data that may be important to a case. It is often difficult to investigate and gather evidence on a confidential basis in a technical computer environment in which possible suspected technologists are frequently required to obtain, preserve, and analyze evidence. It may be necessary to take certain technologists into confidence to assist in this effort. Frequently, a computer operator, maintenance engineer, or computer programmer may be required. The audit department can sometimes be a useful source of such investigative personnel.

It may be advisable under some circumstances to take immediate action with a suspect to minimize loss. In such cases a suspect should be denied access to the areas or resources of the organization where losses could occur until the problem is resolved. In other cases, to obtain sufficient evidence of a possible illegal act, it may be important not to arouse the suspicion of a suspect that investigation is taking place. This should be done with great care and professional guidance.

CRIMINAL JUSTICE AGENCIES PREPARED FOR COMPUTER-RELATED CRIME

In addition to the adoption of specific laws against computer-related crime, many criminal justice agencies are preparing themselves and gaining experience to deal with this new form of crime. Potential victims can have increasing confidence that criminal justice agencies can adequately and expertly deal with computer-related crime. The FBI has trained more than 800 of its agents and accountants in computer-related crime courses provided at the FBI Academy. Similar courses have been offered to police agencies to assist them as well. Police departments and prosecutors' offices are using computers extensively in their work and are becoming familiar with the technology. Many large prosecutors' offices and those located near organizations making extensive use of computers have collectively handled hundreds of computer-related crimes and are rapidly gaining valuable experience. In all of these ways the criminal justice community is preparing to assist the potential victims of computer-related crime.

PRIVACY AND SECURITY DOCUMENTS

Other Publications of NCJISS Privacy and Security Staff

Privacy and Security of Criminal History Information: A Guide to Dissemination
(NCJ 40000)

Privacy and Security of Criminal History Information: A Guide to Record and Review
(NCJ 48125)

Privacy and Security of Criminal History Information: A Guide to Administrative Security
(NCJ 49110)

Privacy and Security of Criminal History Information: A Guide to Audit
(NCJ 59647)

Privacy and Security of Criminal History Information: A Compendium of State Statutes
(NCJ 48981)

Privacy and Security of Criminal History Information: A Compendium of State Statutes
1979 Update (NCJ 59645)

Privacy and Security of Criminal History Information: An Analysis of Privacy Issues

Privacy and Security of Criminal History Information: An Analysis of Privacy Issues
1979 Update (NCJ 59646)

Privacy and Security of Criminal History Information: Users Manual
(NCJ 59644)

Privacy and Security of Criminal History Information: Privacy and the Media
(NCJ 59643)

Privacy and Security of Criminal History Information: A Summary of State Plans

Privacy and Security Planning Instructions
(NCJ 34411)

Confidentiality of Research and Statistical Data
(NCJ 47049)

Confidentiality of Research and Statistical Data: A Compendium of State Legislation
(NCJ 44787)

END