Combating Computer Crime

Prevention, Detection, Investigation

Chantico Publishing Company, Inc.

McGraw-Hill, Inc.

New York St. Louis San Francisco Auckland Bogotá Caracas
Lisbon London Madrid Mexico City Milan Montreal New Delhi
Paris San Juan São Paulo Singapore Sydney Tokyo Toronto

FIRST EDITION
FIRST PRINTING

Published by **McGraw-Hill, Inc.**

Library of Congress Cataloging-in-Publication Data

Combating computer crime : prevention, detection, investigation / by Chantico Publishing Company.
p. cm.
Includes index.
ISBN 0-8306-7664-3
1. Computer crimes—Investigation. 2. Computer crimes--Prevention. I. Chantico Publishing Co.
HV8079.C65C65 1990
363.2'5968—dc20 90-44600
CIP

For information about other McGraw-Hill materials, call 1-800-2-MCGRAW in the U.S. In other countries call your nearest McGraw-Hill office.

Senior Editor: Jerry Papke
Technical Editor: Laura Bader
Production: Katherine G. Brown
Book Design: Jaclyn J. Boone
Cover Design: Lori E. Schlosser

Combating Computer Crime

Prevention, Detection, Investigation

Contents

1

How to use this book

THIS BOOK EXPLAINS WHY A MANAGEMENT PLAN OF ACTION IS VITAL TO the establishment of an effective computer crime prevention program that guards against unacceptable risk while surfacing those risks that are acceptable from a cost/payback view. It describes the options available to senior management in preventing and detecting computer crime. It explains the categories of computer crime threats and examines the strategies available to management to reduce computer crime. Strategies are identified in terms of effectiveness against threats. The end-product of this part is twofold:

- A recommended organizational computer crime policy
- A management level plan of action for implementing that policy

It is designed to identify **computer crime risks**. Procedures are then presented to help organizations identify threats to which the organization is most vulnerable. Several techniques are presented for identifying computer crime vulnerability profiles to illustrate the threats requiring the most attention.

It describes how to **prevent computer crime**. Two options are available for addressing computer crime. The first is to install measures aimed at preventing the computer crime, and the second is using measures that **detect computer crime**. In actual practice, both approaches are necessary. "How to" information is presented for supporting the pre-

vention strategies adopted during the management computer crime plan of action.

The fourth thrust of this book is how to detect computer crime. The standard management and audit functions are not designed to specifically detect computer fraud, but if properly executed, they should detect such frauds over a period of time. Large computer crimes should be easily detected, while smaller ones can be detected through management oversight and audit tests over an extended period. Some computer crime detection methods are introduced, in addition to the emphasis placed on the value of many regular management and audit practices that are beneficial in detecting computer crime. Detection involves investigation, which plays an important part in the uncovering of computer crime.

The science of preventing and detecting computer crime is maturing. Unfortunately, at the same time the enforcement mechanisms improve, criminals are learning new and better ways to defraud organizations. In order to keep the users of this manual current in the new methods of conducting, preventing, and detecting computer crime, this manual will be periodically updated.

Senior management

Computer crime is a responsibility of senior management. While they personally need not be involved in the prevention and detection of computer crime, it is important that they establish an appropriate environment to encourage the prevention and detection of computer crime.

Chapter 2 explains how to establish a computer crime policy and a management plan of action to implement that policy. The material in chapters 3, 4, and 5 provide the necessary background information needed to develop an effective computer crime policy and plan of action.

Senior management should take personal responsibility for developing the computer crime policy and plan of action. This does not exclude assistance by staff personnel. Rather, it implies strong management support for such a policy and plan of action and a personal involvement by one or more members of senior management in the development of that policy and plan.

Operating management

The primary responsibility for the prevention of computer crime resides with operating management. Operating management should also be involved in the detection of computer crime, even though it may not be one of their prime responsibilities. Because operating management is so closely involved with day-to-day events, they are frequently one of the first parties to detect irregularities in computer processing.

Because responsibility for the correctness of computer systems is shared between user and data processing management, there is a shared responsibility for the prevention of computer crime.

Auditors and investigators

The internal and external auditors, investigators, and other assessment-oriented individuals have a primary responsibility for detecting computer crime. Although their investigations may result in recommendations to prevent computer crime, this is a by-product of their investigative work. This does not imply that all auditors and investigatory individuals have a computer crime prevention responsibility but, rather, if the responsibility exists in an organization, it most likely exists with review-type individuals.

Information services department

Information services/data processing personnel implement the controls in automated applications. They are responsible for assisting users in protecting their applications and for creating a computer environment in which it is difficult to commit a crime. In some organizations, the data processing organization may perform much of the computer crime analyses for the users, in which case they will assume some of the user management responsibilities.

Legal implications

According to the *Computer Crime Investigation Manual* by Timothy A. Shaebeck, the legal implications of computer crime are as follows:

> Elements of computer crime: The Battelle study for the Law Enforcement Assistance Administration entitled *The Investigation of White-Collar Crime: A Manual for Law Enforcement Agencies*, defines the five elements of white-collar crime. In general, these five elements can also apply to computer crime. It is important to recognize at the outset that the elements discussed below apply more to the white-collar types of computer crime and not to types of "common" crime, such as arson or burglary.

As stated in the white-collar crime manual, it is important that the investigator and prosecutor of white-collar crime, vis-à-vis computer crime, recognize that these crimes invariably display certain characteristics. It is possible to analyze the execution of these schemes and note that the offenders have certain common objectives. Familiarity with these five elements can serve as a general framework for planning and undertaking action to combat computer crime.

Before reviewing the individual elements, consideration must be given to the possible cycle or recidivist nature of computer crime (see Fig. 1-1). The majority of the computer crimes that are responsible for large monetary losses take place over a period of time and usually require the repeated commission and covering up of an illegal act. Usually, only small amounts of money are embezzled from an organization at one time. However, over a period of time, the amount usually grows (as in the financial industry where computer-related embezzlements average $1.5 million).

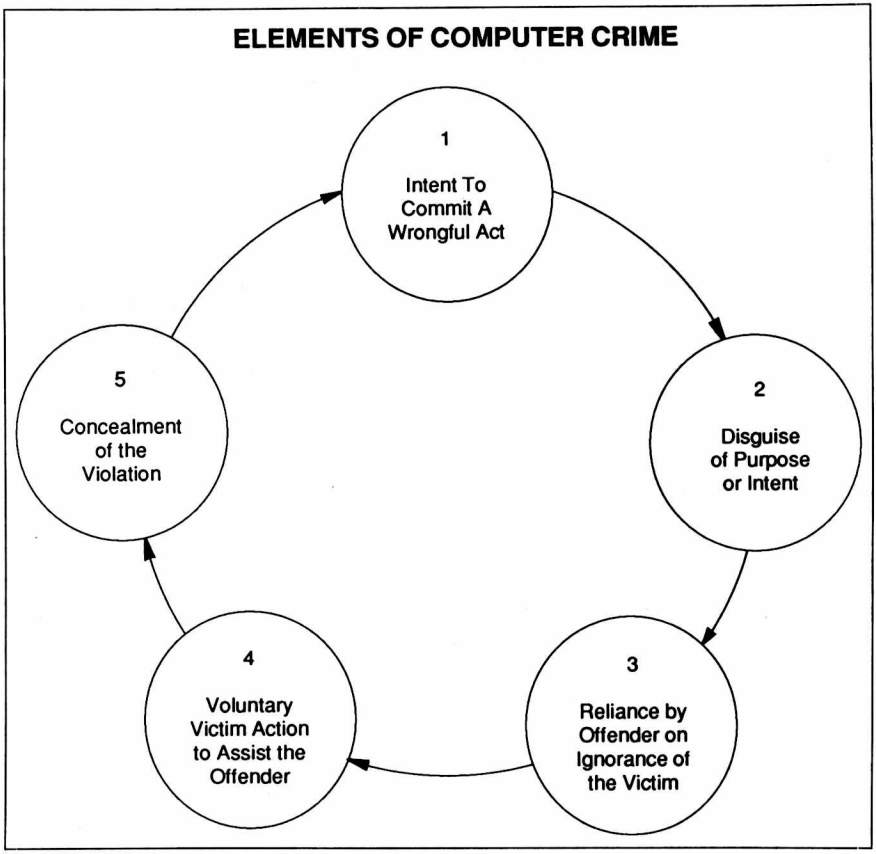

Fig. 1-1. Elements of computer crime.

Elements of computer crime

Intent to commit a wrongful act As mentioned earlier, many of the computer abuse incidents border on the line between unethical and

illegal acts. However, most electronic data processing (EDP) personnel know the essence of the laws that apply to their conduct in their work environment and can be held responsible for their acts. These people usually know when they are involved in a wrongful act, although they may not have an awareness that a particular statute is being violated. Intent involves the presence of some wrongful purpose or objective.

Disguise of purpose or intent Disguise of purpose involves the character of the offender's conduct or activity in the implementation of his plan. He uses disguise to cover up the actions he undertakes to implement his scheme. Disguises can take the form of forged source documents, altered computer input or output, or hidden program routines. Verbal disguise is also usually employed in combination with these items.

Reliance by the offender on ignorance or carelessness of the victim *The Investigation of White-Collar Crime* manual states, "While intent and disguise, the first two elements, are clearly elements which originate with and are controlled by the white-collar offender—involving the offender's own objective and chosen method of execution—reliance . . . on ignorance and carelessness of the victim is a victim-related element, since it is based upon the offender's perception of victim susceptibility. The offender will not go forward unless he feels he can depend upon the inability of the victim to perceive deception."

One of the biggest fears that a computer criminal has is the fear of being caught. In order to avoid this situation, he carefully plans and executes the crime, taking great care to cover his trail to avoid being apprehended.

Voluntary victim action to assist the offender The offender must usually induce the victim to voluntarily undertake some act for his illegal scheme to be successfully completed. In computer crime instances, this may include the following:

- Obtaining management approval to run a test on the organization's accounts receivable system. The "test" is really a disguise for the offender to produce a list of the organization's customers which will then be sold to a competitor.
- Creating fictitious medical claims so that payment checks are generated by the computer, signed by the authorizing personnel, and mailed to the offender.
- One of the early classical cases of computer crime involved MICR encoded bank deposit slips. The offender ordered extra slips from the bank that were MICR encoded with his account number. Upon receipt of these slips, he went to several of the bank's branches and put his deposit slips with blank deposit slips at the counters. Although the bank's customers wrote their own account number on the deposit slip, the MICR scanner only read

the MICR code provided on the bottom of the slip. The perpetrator accumulated $250,000 in 4 days from other people's deposits. He then withdrew $100,000 from his account. He has never been apprehended.

Concealment of the violation It is important for the computer criminal to conceal his illegal acts in order to be able to continuously repeat his crime and, of course, to avoid being caught. It is a well-known fact that the best computer fraud schemes will probably never be detected. In fact, about 95 percent of the computer crimes that have been uncovered to date have been uncovered purely by accident, not through investigation.

Concealment is important to the computer criminal because he usually works in the open as an employee of the organization. Due to the nature of the computer and its processes, concealment can be quite easy, especially in the remote terminal teleprocessing environment. Manipulation of accounts via a remote terminal aids in concealing the identity of the offender.

In addition to the assault from the outside, computer professionals must take into account the violations of law that can occur within their own company and cause them to become computer criminals. Several large corporations have been successfully sued for copyright violations. For example, Lotus Development Corporation sued Rixon, Inc., for $10 million because Rixon copied and distributed Lotus 1-2-3 to its branch offices. Since then, Lotus has also sued The Health Group in Nashville, Tennessee, for over $1 million. With this kind of precedent, it is important for managers to ensure that their employees do not violate copyright laws.

Most of the examples of computer crime presented deal with large computer systems. However, the proliferation of micro- or personal computers has accelerated the incidence of computer crime, both because the number of computers available to attack has increased, and because there are more computer-literate people capable of committing these crimes. Therefore, it is incumbent upon all levels of computer professionals within an organization to support the computer security effort. In this book we will explore the methods of support that have worked in other companies in hopes that they will provide additional ideas for the computer professionals of today.

2

Developing a plan of action

THE PREVENTION AND DETECTION OF COMPUTER CRIME ARE IMPORTANT responsibilities. The fulfillment of these responsibilities involves the development of a computer crime policy and a plan of action to implement that policy. The growing threat of computer crime makes it difficult for any computer owner to avoid addressing this potential threat.

This chapter describes the magnitude of the threat of computer crime. It also describes the need for a computer crime prevention policy, how to develop such a policy, and the process of developing a plan of action for implementing that policy.

Classes of computer crime

Computer crime is crime against an organization or individual in which a computer is involved. The Equity Funding Insurance Company fraud in the late 1970s was the first highly publicized example of a crime involving a computer.

The commonly accepted definition of computer crime is a **"crime against an organization in which the perpetrator of that crime uses a computer for all or part of the crime."** This is a very general definition, but we know that the computer can be used as a tool to help commit a crime, or the data within the computer can be manipulated to result in a loss to the organization. The two classes of computer crime are fraud and abuse.

Of the two terms (fraud and abuse), *fraud* is the only term with a precise, legal definition. It is defined as "obtaining something of value unlawfully, through willful misrepresentation." It is an intentional perversion of truth designed to induce another to part with something of value. The key aspects of fraud are that it is intentional, it is unlawful, and there is an element of misrepresentation. An example of fraud is a physician who submits a claim for reimbursement under medical insurance for a service he/she knows was never performed.

The following are definitions of computer fraud and computer crime:

> "*Computer fraud* is any defalcation or embezzlement accomplished by tampering with computer programs, data files, operations, equipment or media, and resulting in losses sustained by the organization whose computer system was manipulated. In most instances, this would encompass all activities in the computer department, as well as those departments that directly enter or prepare computer input." Brandt Allen, "The Biggest Computer Frauds." *Journal of Accountancy*.

> "We define *computer-related crimes* as acts of intentionally caused losses to the government or personal gains to individuals related to the design, use, or operation of the systems in which they are committed. Computer-based data processing systems are comprised of more than the computer hardware and the programs (software) on which they are run. The systems include the organizations and procedures (some manual) for preparing input to the computer and using output from it. Computer-related crimes may result from preparing false input to systems and misuse of output, as well as more technically sophisticated crimes, such as altering computer programs." *U.S. General Accounting Office*.

Abuse is the improper use of resources provided by an organization to the individual who misuses those resources. The key aspects of abuse are that it is intentional and improper, but it does not necessarily imply the violation of a specific law or the presence of misrepresentation. In theory, any conduct or activity that is fraudulent will also be abusive. When an individual commits fraud against an organization, the individual is abusing the organization's programs. Examples of abuses that are not fraudulent are an employee who makes excessive telephone calls from his office phone, or a computer user who uses a company computer for personal business or financial gain.

Computer fraud and abuse both involve the intentional and improper use of the computer, but fraud also implies the violation of a law or the presence of misrepresentation. Obviously, abuse is much harder to diag-

nose and prove than fraud; but in actual practice, computer abuse may be much more costly to organizations than computer fraud. Fortunately, the same measures that prevent and detect computer fraud are also effective against computer abuse.

The true definition of computer abuse is more difficult to pin down. In general, any abuse will involve the unauthorized use or manipulation of computer equipment and often the data contained within that equipment. Some additional examples of specific types of abuse will clarify the definition.

Storing personal data on a company machine can be considered abuse, for it consumes valuable storage resources. On the other hand, a much more serious type of abuse can involve the theft or destruction of data. In the case of Donald Gene Burleson of Fort Worth, Texas, the abuse took the form of a logic bomb left in the company's computer after his employment had been terminated. When the bomb went off, it destroyed 168,000 sales commission records. The loss of this data was unrecoverable and Burleson was convicted of "harmful access." This represented the first time a computer user was convicted in an abuse case.

Another widely publicized example of massive computer abuse was the virus released over many networks by Robert Morris, Jr. It has been determined that this virus cost many millions of dollars to clean up, and it was designed as a harmless virus! Like Burleson, Morris was convicted of misuse of a computer.

There is a third class of computer crime which is spreading like an epidemic across the computer community and does not fall neatly into either the fraud or the abuse category. This is the theft of computer software through illegal copying. Software piracy is considered the most common and most expensive type of computer crime. Although many people feel that stealing software is a personal matter, the liability of both the individual and the company whose employees are stealing copyrighted software must be examined.

Examples of computer crime

In the preceding chapter we looked at some specific examples of particular computer crimes which illustrated class distinctions. However, the spread of computer crime has touched nearly every form of occupation. It is estimated that within 10 years all crimes will involve the computer in some way. Currently computer crime breaks down into six major areas. Listed below are each of those areas and their related percentages:

- Trespass, 2%
- Theft of services, 10%
- Alteration of data, 12%
- Damage to software, 16%

- Theft of information or programs, 16%
- Theft of money, 44%

(Source: National Center for Computer Crime Data.)

Looking at this list, it is obvious that no one is safe from some form of computer attack. The attack may take the form of simple trespass, or it may be a more insidious invasion via some sort of destruction software such as a virus or Trojan horse.

It would be foolish to assume that the computer user is always the target of the crime and not, at times, the perpetrator. Software piracy has reached epidemic proportions across the computer community. Looking at the numbers, it seems safe to say that most personal computers in homes and businesses today have at least one "hot" program in residence. It may be a shareware program for which the user has yet to pay, or it may be a more blatant "borrowed" copy of a game or utility. Software developers have determined that for each copy of a software package sold, between one and three illegal copies exist. Sometimes this form of crime takes on almost laughable proportions. Studies of college students have found some with hundreds of stolen programs amounting to millions of dollars.

It is also common for a company to buy one copy of a business program and then copy it across all the machines in the company. This form of computer theft has recently been the target of extensive litigation. The personal computer software publisher Ashton-Tate, in the person of Geoffrey A. Berkin, is suing several major corporations who have illegal copies of some popular business programs such as dBase III.

Other examples of major computer crimes include:

- Rebecca Doyle, who owned a title company in St. Petersburg, Florida, and was once named American Businesswoman of the Year, was charged with embezzling $2 million using a computer.
- In 1985, American Brands Co. paid an undisclosed amount to Micropro International Corporation and Association of Data Processing Service Organizations Inc. through an out-of-court settlement of a software piracy claim. American Brands admitted some of its employees had stolen copies of programs such as WordStar, a Micropro program.
- For over a year an intruder had free access to the data files of over 36 U.S. military research computers. This intruder was working from his home in West Germany, picking out data on the Strategic Defense Initiative and other defense-related topics. If it had not been for the curiosity of Clifford Stoll, a manager of computer systems at the Lawrence Berkeley Labs in California, this hacker might still have free reign of those computers.