Halting Computer Crime and Abuse: Management’s Newest Challenge

Karen A. Forcht, Information Sciences, James Madison University, Harrisonburg, Virginia
Joan Pierson, Information Sciences, James Madison University, Harrisonburg, Virginia
Ben Bauman, Information Sciences, James Madison University, Harrisonburg, Virginia

Abstract

As computers enter the business environment with increasing regularity, their introduction is also coupled with paramount abuse. This paper explores the profile of the typical computer criminal and describes some of the most commonly used methods for violating a computer system. Included in the discussion are: data dilling, trojan horse, salami technique, superzapping, trapdoors, logic bombs, synch attacks, scavenging, data leakage, piggybacking or impersonation, wiretapping, manipulation, and viruses.

Introduction

In recent years, computers have become a very integral part of modern society as they speed up operational tasks, simplify our jobs, organize information, calculate numbers, and generally aid in processing the large volumes of data and information that are vital to the success of our organizations. At the same time, computers have confused, intimidated, and, in all too many cases, been violated. The integration of computer systems into our business and personal lives has occurred so rapidly that many people do not fully appreciate (or comprehend) the benefits of automation. Since a reasonable "comfort level" has not been achieved by many people, it is difficult to fully appreciate the "potential for harm" that computers can generate. As is so often the case with many inventions or innovations, the propensity for good is too often coupled with the "flip-side" - potential for harm.

What Is Computer Fraud And Abuse?

In the most simplistic terms, computer fraud can be defined "as the abuse of a computer whereby the victim suffers from the wrongful intentions of a perpetrator." To fully understand the term, certain aspects must be examined and explained. Computer fraud, being a relatively new concept, has emerged as a direct result of the increased use of computer systems for storing data. Almost in direct proportion, as a firm increases its use and dependence on computers, the potential for harm or misuse increases correspondingly. The National Center for Computer Crime Data in Los Angeles, California, in its recent publication entitled, "Computer Crime, Computer Security, and Computer Ethics," states that "by increasing the number of people with access to computers, you increase the number of potential criminals." According to Joy Bloomecker, Director of NCCD, the portion of our labor force involved with computers has been growing for quite some time and it gives no indication of starting to stop. When a company stores all of its important data in computer data banks and does not properly safeguard this vital company asset, then the potential for vulnerability is paramount. All types of organizations utilizing computers are potential victims.

Statistically, banks appear to be the hardest hit -- possibly due to the immediate cash advantages of "ripping off" a financial institution. Experts believe that the large amounts of money and transactions in the banking industry make it the most likely target for computer crime -- a modern day Bonnie and Clyde scenario.

Who Is The Typical Computer Criminal

When analyzing computer fraud, a profile of potential criminals must be understood. The perpetrators' methods of fraud, statistics on damages done, and the methods of prevention must
be fully explored in order to grasp the magnitude of the dilemma facing society and businesses today.

If we were to conjecture that the "typical" computer criminal's profile was six feet tall, has dark hair, wears navy blue three-piece suits, and works as a computer programmer, our identification task would be quite simple. In reality, however, compiling a profile is not that easy because the representative sample necessary for observation is not always available due to the relative "newness" of the profession of computer crime. Since our historical perspective is limited, long-term patterns are not measurable. The National Center for Computer Crime Data offers some insight into the "typical" computer criminal as being: between 13 and 51 with the average age being 22, and most likely employed as a programmer, input clerk, is a student.

John Sheridan in his Industry Week article, "Is There a Computer Criminal Working for You?" offers some further profiles as: (1) able to pass pre-employment screenings with "flying colors", (2) usually young - between 18 and 30, (3) an amateur -- having no previous criminal record, (4) usually male, (5) bright, highly motivated, and adventurous.

Generally speaking, computer criminals are ordinary people with a problem to solve and are in a position of trust in their organizations. Many of the same characteristics that make them highly desirable as computer specialists also make them fit the profile of the computer criminal. Employers must be aware of this "matching" and use rigid pre-employment testing, as well as periodic reviews about job satisfaction. Job dissatisfaction has been shown to be a strong motive--either from boredom or for revenge. The criminals may often rationalize their actions with the "bloodless crime, no-smoking gun syndrome"--no one is being harmed--the only damage is to a large, uncaring, impersonal corporation.

According to James Martin and Adrian Norman in The Computerized Society, the employees who appear to have the greatest ability, due to their positions, in "covering up" their crimes are: programmers, managers, bank clerks.

To attempt to determine just who will become the next criminal is truly not an easy task as it does not always hold true that only those with easy access or computer knowledge will be most intent on breaking into the system. There does not appear to be a single answer or a "quick fix" in terms of detection or prevention, thus various methods will need to be considered.

How Do They Do It?

To better understand just how these crimes are committed, a few of the classic methods need to be discussed. Even though these scenarios vary from time to time and from instance to instance, many criminals today are employing some variation of the "tried and true" methods that have succeeded in the past. Some of the classics are: data daddling, trojan horse, salami technique, superzapping, trapdoors, logic bombs, asynch attacks, scavenging, data leakage, piggybacking or impersonation, wiretapping, manipulation, and viruses.

Data Daddling

Unauthorized changing of data BEFO RE or DURING input into a computer system

Changes can be accomplished by anyone who has access to the data. Daddling is the safest, simplest, and most common method of computer crime used today. An example could be a time-keeping clerk who completes data forms of hours worked by employees. The computer, internally, only processes numbers, whereas externally, all records are kept by name. The clerk fills out overtime cards on employees who frequently work overtime hours, yet inputs the hours into his/her own employee number when entering the data into the computer, thereby increasing his/her income several thousand dollars each year.

Trojan Horse

Computer instructions secretly inserted in a computer program so that when executed, unauthorized acts are performed.

This method tends to be commonly used for intentional computer-based fraud and sabotage as instructions can be inserted and removed so that no evidence remains. There is virtually no trace left -- a perfect "no fingerprint" crime.
Salami Technique

Unauthorized covert process of taking small amounts (slices) of money from many sources.

The most common salami slice is the "round-down" fraud. For example, when figuring interest rate calculations, the fraction of one cent that is normally rounded up or down to the nearest cent is put into the criminal's own account. Rather than distributing the rounded down remainders to the individual accounts as they build up, the amount is accumulated into a separate account. The accounts will still balance but over a period of time a sizeable amount can be accrued.

Superzapping

Unauthorized use of utility computer programs that violate computer access controls to modify, destroy, or expose data stored in a computer.

This term is derived from superzaps which is a macro utility program used in most IBM computer centers as a systems tool. A universal access code is needed in computers for various reasons and can be compared to a master key that is used when other keys are lost or misplaced. An instance of superzapping occurred in New Jersey when a computer operations manager was using a superzap procedure to make changes to account balances to correct errors as dictated by management. He soon learned that he could use this superzap process to his personal benefit and transferred funds to three friends' accounts. He was eventually caught only because a customer's complaint led to an investigation.

Trapdoors

Functions, capabilities, or errors in a computer program that facilitates compromise or unauthorized acts in a computer system.

When developing computer programs, it is often necessary to insert debugging aids that provide breaks in the program for insertion of additional code and intermediate output capabilities. Trapdoors then make modification of the program easier and are usually eliminated at the end of the program. When trapdoors are used for unauthorized purposes, they are referred to as "negative specifications." Recently, this method was discovered in a commercial time-sharing computer service. The programmer, with the aid of a user of the time-sharing service, was able to use large amounts of computer time free of charge and obtain data and programs of other time-sharing users.

Logic Bombs

Taking advantage of the asynchronous structure of computer operating systems to perpetuate an unauthorized act.

A computer normally performs requests asynchronously based on resources available rather than in the order they are received. Asynchronous attacks are highly sophisticated methods of confusing the operating system to allow it to violate the isolation of one job from another. Violating or overriding priority codes is a popular use of this method.

Scavenging

Similar to a scavenger hunt where random, loosely defined items are collected.

Scavenging is a covert, unauthorized method of obtaining information that may be left in or around a computer system after the execution of a program. This scavenging can include both a physical search and a search for residual data within the computer storage areas.

Data Leakage

Unauthorized covert removal or detaining copies of data from a computer system.

Several ways that data leakage can be accomplished are: (1) sensitive data may be hidden in otherwise innocent looking reports, (2) interspersing data, (3) encoding data to look like something different, and (4) controlling and observing the movement of equipment parts.

Unlike many computer violations which are initially "innocent," data leakage acts are deliberate and not unintentionally or accidental.

Piggybacking and Impersonation

Gaining unauthorized physical access to guarded
areas when control is accomplished by electronically or mechanically locked doors.

Electronic piggybacking occurs when a computer or terminal covertly shares the same communication line as an authorized user. Impersonation occurs when one person falsely assumes the identity of another. An example of impersonation that has been recently reported was an individual who stole electronic funds transfer (EFT) cards and then contacted the owners. Posing as a bank official, the person then requested their personal identification (PIN) numbers. The card owners were lead to believe that the bank was attempting to prevent a theft from gaining access to their accounts.

Wire Tapping

Interception of data communication signals with the intent of gaining access to data transmitted over communications circuits.

As more and more computer systems are tying into networks, wiretapping's potential could become the newest "nightmare" of computer crime. In the past, wiretapping was deterred a great deal by the expensive equipment required. With the price of modems and communications equipment becoming financially feasible, however, this method of theft could easily be within the reach of many people all too soon.

Manipulation

Computer is used as a tool for planning, controlling, and monitoring a crime.

While both of these techniques are somewhat sophisticated by design, they are well worth the efforts of the ardent, dedicated criminal. Simulation attempts to create (or simulate) as closely as possible a real-life situation, i.e., a company's operation. Modeling, somewhat different in design, attempts to recreate (usually in smaller form) a real entity, i.e., robots, model airplanes. There have been several documented cases where the computer has been used in insurance companies to "model" their operations and determine the effects of the sale of large numbers of insurance policies -- a type of "what-if" game. By playing around with the numbers and creating hundreds and thousands of fake insurance policies, companies were virtually "wiped out" when benefits were paid to "non-existent" policies or premiums were paid only "on paper" on supposedly valid policies.

Viruses

Changes the volume label of a start-up floppy disk or hard disk so that each time it is run, it "infests" disks inserted later.

This winter, at Lehigh University in Bethlehem, Pennsylvania, a virus started destroying data on floppies and hard disks were irretrievably wiped out. Other viral outbreaks recently occurred at the University of Delaware, Georgetown University, the University of Pennsylvania, the University of Virginia, and a Martin Marietta research facility. So far, damage has been limited to university computers and research facilities. But there is nothing inherent in the nature of the virus that would prevent it from affecting information systems in many commercial offices.

Conclusion

Jay BloomBecker's predictive statement that "like any other type of crime, computer crime will ultimately reflect the culture that surrounds our computers. Looking at the "culture" of computing is not an encouraging exercise." Computing is a new frontier and as in any "new territory," quick profits, bold gambles, and little concern for the long run seem often to be the norm.

It is becoming increasingly obvious that there are many methods or tools that can be (and are) used to perpetrate computer-related crimes. Each time a new application or technology is introduced, a new method is added to the criminal's list of ways to circumvent the system. Companies and society must remain constantly on guard, cognizant of the fact that we can never fully eliminate computer-related crime. Hopefully, through close monitoring of our systems, encouraging ethical codes, and increasing legislation to prosecute criminals, we can be reasonably assured that the privacy, validity, and integrity of data is maintained.

John Naisbitt in his best-selling book, Megatrends, challenges the computer profession by projecting that "the new source of power is not
money in the hands of a few but information in the hands of many." If we are to feel as if we are in control of this wealth of information, much time, thought, effort, and financial resources must go into guaranteeing the "safeness" of our most valuable asset—information. The challenge is a clear-cut one and must be met head on. Only then, can we truly say that computers are indeed a valuable tool to business and individuals.

References


Continued from page 90