Computer Crime: Insecurity in Numbers

As computer networks proliferate, businesses and other institutions may be leaving valuable information vulnerable to fraudulent, wasteful and criminal acts

By IVARS PETERSON

Brooks Photography & Graphics by Jerome Demura

The computer is an innocent who will reveal anything it knows, provided it is asked in the right way. By manipulating its digital psyche, a person can create, destroy, divert or change information. Anyone can steal something from a computer's memory yet leave the valuable behind and show no trail.

As computer networks increasingly interlace society's fabric, more and more organizations and individuals entrust their most valuable possessions — information and money — to computers. And, increasingly, they are getting burned. Students have altered grades, bank employees have shifted pennies from customer accounts into personal hoards, government workers have used or sold sensitive information, and many have taken free rides by stealing computer time for their own purposes.

A recent report from the U.S. General Accounting Office says computer information systems in government agencies "are highly vulnerable to fraudulent, wasteful, abusive and illegal practices." A clerk manipulated input information at a Department of Transportation computer to steal more than $800,000. Similarly, the Social Security Administration lost more than $500,000 in disability benefit funds. Internal Revenue Service employees obtained refunds by preparing fraudulent income tax returns for input to a computer. At least 30 employees had unauthorized access to the Department of Agriculture's computer and data files. "Some used the computer to perform outside consulting work, to gain access to and use proprietary data, and to make unauthorized and premature disclosure of information considered by Agriculture to be highly sensitive," says the report.

Computer data systems often contain a high concentration of valuable and sensitive information, such as a corporation's mailing lists and customer accounts, and the government's income tax data. This information is susceptible not only to deliberate attack but also to errors. In large amounts of data, errors are very difficult to discover and correct.

Large computer systems need a reasonable level of protection. However, few company executives and government agency officials understand how to provide that protection. Leslie D. Ball of Babson College in Wellesley, Mass., writes in the April 1982 TECHNOLOGY REVIEW, "Industrial security and bank security are fairly well understood, but computer security is not." Managers know that sensitive papers should be locked up, but they are often less able to grasp how to secure electrons flowing in wires or electromagnetic waves traveling across the country. In addition, new technology creates new problems. As word processors replace typewriters, these small computers (sometimes connected to a company's central computer) are easy to misuse. Typewriters don't store information once a report is finished; word processors keep the data on file in the system.

Robert S. Gordon, executive vice president of Burns International Security Services, Inc., said in his keynote address at the 1982 Carnahan Conference on Security Technology, "New computer systems are reaching the market so quickly that security for these systems is almost an afterthought."

Many people still imagine a company's computer as a set of large metal cabinets with whirling magnetic tapes and flashing lights, punched cards and display screens, all collected in one large, air-conditioned room. In the past, computer security consisted of protecting this computer room by using guards, elaborate locks, magnetic card identification and other physical means. If the computer room was inviolate, then so was the computer. In institutions like universities, often the security arrangements were minimal, if they existed at all.

Computer systems now are quite different. Terminals, which may be scattered throughout a building or around the world, are interconnected in complicated networks. Telephone lines and satellites transfer messages from one computer to another. Citibank, for example, electronically processes more than $30 billion a day for its customers. Its 200 branches in 100 countries are linked by telephone lines with major switches in Hong Kong, London, Bahrain and New York. An error or a theft potentially can have an enormous price tag.

These networks can be vulnerable in surprising and unexpected ways. At the Dalton School in New York City, four 13-year-old students used a classroom computer and telephone line to break into a Canadian data network and gained access to the files of 22 companies. In another case, a group of teenagers found discarded systems manuals in the trash bins behind a company's building and obtained enough information to shut down the company. In Chicago, two high school boys reached the DePaul University computer by telephone. Their home computer randomly generated thousands of possible master account codes in a matter of seconds until they found a code number allowing them into the university's computer. By changing all the master codes, during their romp through the computer, they prevented the university from using the system for a week.

Unauthorized computer hitchhikers have used ARPANET, the Defense Department's computer network for research and development contractors, for passing along messages and playing games. Friends who had access to terminals in the network often provided the needed telephone numbers and passwords. In a widely publicized incident earlier this year, students at the University of California at Berkeley were credited with discovering a flaw in a computer operating system that allowed a user at one terminal to trick the computer into thinking he was another user working at a different terminal. Thus, he could browse through anything to which the other user had access.

The security problems and needs in computer networks are dramatically different from earlier concepts of computer protection. Safeguards written into computer programs and the use of encryption and secret codes, in a sense electronic fences, become more important than physical means of protection. Now, security experts speak of "information systems security," because the entire system, including all its links and terminals, must be considered.

There are more than 100,000 computer sites in the United States and Europe that are constantly talking to one another — transferring funds, transmitting critical data. The United States has more than 3 million computer terminals, many of which have access to central computer files. More than 500,000 personal computers have been sold. Add "intelligent" office machines like word processors and automatic tellers at banks, and the poten-

tial for abuse seems very high.

How extensive is the problem? No one knows.

Computer-assisted crime is recognized as a real problem, but actual losses are difficult to estimate, says Oliver R. Smoot of the Computer and Business Equipment Manufacturers Association. Some estimates set losses as high as $5 billion per year, while others put them as low as $300 million annually.

"The statistics are so bad that we really know very little about it," says Peter Watkins of the auditing firm Peat, Marwick and Partners in Toronto. Much of the evidence is anecdotal, and experts disagree in many cases over whether a computer was an essential element in the crime. An auditing firm reports that in 1980 in the United States, only 75 true cases of computer-assisted crime occurred among approximately 350,000 computer installations for a loss of merely $40.3 million. For many analysts, this represents just "the tip of the iceberg" because many companies may be reluctant to admit their losses publicly, but there is no way of judging the percentage of unreported crimes.

Despite uncertainties about the extent of computer-assisted crime, a strong feeling exists that the number of crimes is increasing. One reason, some experts say, is that a computer crime is easy to accomplish and hard to detect. A former Federal Bureau of Investigation official estimates that the odds are only one in 10,000 of a computer criminal going to jail. In one case, the Equity Funding Insurance Co. fabricated 64,000 phony policies worth $1 billion, which were sold later to reinsurers. The loss was $27.25 million. When caught, the perpetrators had a computer program available that could have erased all the computer evidence.

An increasing number of employees are gaining access to computer terminals in offices. Smoot says, "The largest continuing area of losses from information systems is from authorized users who abuse the authorization." Contrary to the perception of many people, clerks, administrators and managers rather than data processing professionals and computer experts are much more likely to commit crimes using a computer. "You don't need to know anything about a computer to make a good living as a criminal," says one security expert. Even the teenagers involved in many of the more widely publicized computer-abuse cases were not particularly knowledgeable and used relatively simple techniques.

Smoot says that because the news media tend to play up dramatic crimes that involve computers, however indirectly, the public perceives computer systems to be more vulnerable than they are. Watkins says many losses have occurred simply through bad business practices and controls.

The level of security needed for a given computer system depends on a number of

Illustration by Donna Ward

things: the type of information processed or stored and its sensitivity; the environment and facilities in which the system operates (for example, whether in a university research laboratory or one of the Defense Department's classified computer networks); the nature of the equipment and its telecommunications links; the computer programs (software) used; and the people involved. An analysis is necessary to determine the system's vulnerability to natural disasters (like fire or earthquake), human error and criminal use. Using this information, an organization can select the appropriate combination from more than 300 types of security controls now available. Watkins says, "For a reasonable amount of money, you can get a pretty high level of security."

One way to help prevent illegal use of a computer is to include safeguards within computer programs that operate a system. These include recording who uses the system, for how long and when, and searching for unexpected use patterns. Programs may also include instructions that restrict computer users to those files for which they are authorized, as defined by special passwords or access codes. In the past, programmers put in few safeguards. They had enough problems just getting their programs to work.

Alan E. Brill of Yourdon, Inc., emphasized at a recent national computer security and privacy symposium that programmers need to build in controls and data checks when programs for specific applications are first developed. In banks, for example, various techniques, embedded in computer operating systems, can be used to flag excessive activity or particularly large transactions and reactivation of dormant accounts.

Auditing programs can compare files stored in computer memories for discrepancies, or computer programs to find alterations. They can check for telltale signs like payments to post office boxes, duplicate payments, inventory adjustments and many other activities that possibly signal wrongdoing.

The cost of such software measures is in time. Added controls may delay a computer's response by seconds, which for thousands of transactions daily can add up to a considerable amount of lost time.

Computer networks are vulnerable when electronic information is transmitted along telephone lines or in the air. One solution is to code or encrypt the information so that only those with "keys" can unscramble the data. One example is the Data Encryption Standard, now commercially available (SN: 10/17/81, p. 252). Such systems are used to transfer about $400 billion around the nation each day. Codes can also be used for protecting stored data (SN: 5/22/82, p. 346). Even personal computer owners can now buy encryption devices to keep their private affairs private.

A study from the University of Minnesota reports that most companies could not function properly without their computer systems for more than 4.8 days. Destruction of computer facilities or programs, whether accidental or deliberate, can have a devastating effect. Planned redundancy in computer files, programs and equipment is a high priority as a check on errors and to prevent irreplaceable losses. The Dalton students, in their "prank," were able to erase sufficient data to cause serious problems for two Canadian companies because backup information was not available.

At the computer security symposium, Lt. Cdr. William A.J. Bound, on leave from the Royal Navy to work at the Defense Department's Computer Institute, described an incident in which a sailor "destroyed the operational information, the backup information and the backup backup information" stored in a ship's computer. Consulting the system manual and writing new programs, a team of computer experts on board were able to "circumvent all the necessary controls and...managed to get back almost 100 percent of that information," simply because the sailor hadn't wiped out everything.

One of the dilemmas in the field of computer security is how to determine the effectivness of the security. If nothing happens, either the security system is doing its job, or it may not even be necessary. Who knows?

The Defense Department has several worldwide computer networks, for military command, intelligence services and research and development data, operating at different levels of security. A large number of information sources feed many distribution points where the data are used. Few of those information sources would like their data to go to the wrong place. The department is looking for new ways of ensuring the security of its networks.

Steven T. Walker of the Defense Department told the computer security symposium that the department wants a "trusted" computer system, one that would contain enough controls to allow simultaneous use of many levels of sensitive data, yet not allow unauthorized users access to certain information in the system. This would avoid having to set up different networks for different types of uses, or requiring all users of a system to have sufficient security clearance to handle the most sensitive data likely to be encountered.

As part of its "computer security initiative," the Defense Department established in July 1981 a Computer Security Center at the National Security Agency. This center evaluates commercial computer systems and products and publishes an "evaluated products list" that describes how secure a product is and the kind of environment in which it would be suitable.

The aim, Walker said, is to get trusted computer systems from manufacturers without having to order a system specially designed for the department. In other areas, custom-made products have turned out to be very costly. "We recognize that the only way we're going to get that is if a broad spectrum of the [business] population wants it in addition," Walker said. This means making businesses more aware of security problems so that they will want the products. "When we all ask for the same kind of features from our manufacturers, they will try to provide those features, and we'll be able to get them at a reasonable cost," Walker said. "We recognize that there is an essential education process that needs to go on here."

The DOD Computer Security Center is now evaluating several products and recently issued its first product evaluation bulletin. This product, the Secure Communication Processor (SCOMP) developed by Honeywell Information Systems, Inc., may be the first to meet the requirements of "trustworthiness." About 50 people work at the center, and it has room to grow to 150 or so. "The department is taking a very serious view of the problem and assigning some very competent people to it," said Walker.

Most experts agree that losses will occur from any system, no matter how secure. Although even small computer systems often have sophisticated rules and manufacturers offer security packages that include passwords and controls on access to files, users frequently find the rules more trouble than they're worth to implement. Workers leaving for lunch or a break sometimes fail to turn off computer terminals, leaving them available for anyone to use. Occasionally, lists of passwords or instructions, often relatively simple and easy to remember, are taped to terminals to save bother. One company bought an encryption system and then used the coding key given as an example in the manual to encrypt its messages.

In many cases, common sense and good business practices can prevent or catch many computer-related crimes, abuses and errors. The amount worth spending on computer security depends on the perceived value and risk of potential losses from the company's computer vaults.

John C. Taber, a systems programmer with IBM Corp., has written, "A computer is just a technique or method by which people are doing the same types of things that have been done in the past—embezzlement, thefts from their employers, and so forth. The computer merely gives certain people with knowledge and access an increased opportunity to do this sort of thing and in some situations the opportunity to do it in a greater way than it would be possible with the normal embezzlement and other criminal techniques."

In the end, the human element is the ultimate weakness. "There is no absolute security," says Smoot. The most effective way to break into a secure computer system is with a bribe, he says, or by introducing a pretty woman or a handsome man to the right computer operator. □