WHAT IS COMPUTE SPICL AND WHY DOES IT CONTINUE?
WHAT IS COMPUTER CRIME AND WHY DOES IT CONTINUE?

Falling prices and rapidly increasing technology have made day-to-day use of the computer commonplace in today's business world. The invaluable services of the computer are readily available to everyone from corner grocery stores to international corporations. Unfortunately, with this rapid increase in use, an equally rapid increase in abuse is occurring—computer crime. Computer crime is a major problem all computer users must protect against if reliance on the computer is to continue. To understand the importance of protection, one must understand what computer crime is, the types of crime occurring, why it continues, and what can be done to stop it.

WHAT IS COMPUTER CRIME?

Computer crime has been defined as "any illegal act for which knowledge of computer technology is essential." The computer itself commits no crime. It is a tool used, in lieu of guns or bombs, to complete a coup. The computer only assists criminals. Therefore, it is necessary to protect one's computer from being the key in aiding a thief.

Computer crime differs significantly from any other type of crime. There is often no sign of entry, no fingerprints, no tangible objects missing, oftentimes, no clues at all. The criminals themselves are different. They have new methods of stealing, different lifestyles, and oftentimes are no where
near the scene of the crime. They can enter silently from a remote terminal with the touch of a button. Computer crime is a unique method of crime whose potential severity must be understood before it can be stopped.

Judicial attacks.

Computer crimes are hard to detect and criminals equally hard to catch. If a criminal is by chance caught, the present laws provide little help in prosecuting them. Only a limited number of states have statutes dealing specifically with computer crimes. Most cases are prosecuted under wire tapping. Few crimes are even detected. Most crimes are detected accidently. If detected, only 1 in 30 crimes is prosecuted. Additionally, only 200 individuals worldwide have the technical training necessary to investigate those crimes reported. The problem of prosecuting computer criminals is impeded further by the attitudes of the people in the judicial system. Computer criminals, if convicted often receive small fines and suspended sentences. Many computer criminals are white collar workers, not the typical hardened criminal. Consequently, he receives sympathy from both the judge and the jury. Many jurors do not find the criminal at fault; rather, they blame the victim for leaving themselves vulnerable to the criminal. The fact is that these criminals are as guilty as an ordinary burglar. They are breaking into a computer system, trespassing and stealing another’s property.

It is obvious that victims of computer crime find little reward in reporting these criminals to authorities. If a crime
is discovered, it is most likely dealt with internally. No public report is made. Victims, especially banks, fear the loss of public confidence if a weakness in their security system is exposed. Others do not wish the present vulnerability of their system advertised to other would-be perpetrators. Still others are afraid that competitors may learn trade secrets if the stolen information is revealed as evidence in a trial. Unfortunately, until the judicial process catches up to the rapid advancement of computer technology, it is the responsibility of computer users to learn to identify computer criminals and protect their computer systems from them.

Types of computer crimes.

There are many types of computer crimes users should be aware of. External threats consist primarily of hackers—young individuals who make a hobby of breaking into computer systems. They are treated as white kids rather than as criminals. Consequently, hackers continue to work hard to break into systems. However, thieves external to an organization are not as large a threat as an internal thief can be.

Internal thieves are not typical of or similar to any other type of thief. They do not fit the criminal stereotype. They are trusted employees of the companies they plunder. They are “bright, young and motivated people, energetic and ambitious, the kind personnel directors love to hire.”

Typical crimes include: financial rip-offs, diversion of property and theft of information. These prime employees commit crimes for a variety of reasons: split, revenge, profit, and
even boredom. Individuals who are over-qualified for their positions often find ways to occupy their time. If they have access to information, temptation oftentimes overcomes an otherwise honest employee. Most acts of crime occur while employees are engaged in their daily duties. Individuals in a position of trust are especially susceptible to the temptation to steal.

Internal theft has been reported most often in the banking industry and the government. The government has been plagued by frequent security breaks. The major concern now is that someone could break into top secret information. The government denies the possibility but has beefed up security none the less. Banks are hardest hit by employees utilizing a technique labeled the salt. Customer accounts are debited or credited for small amounts, then deposited in the thief's account. Since a small amount is taken each time from a variety of sources, audits typically do not detect the irregularities. Only a few customers detect the error and question the bank's accuracy. For example,

A teller at the Union Dime Savings Bank in New York used a supervisory program to alter customers' accounts. If any depositor complained of an incorrect balance, the teller moved money from other accounts to the customer's. Routine audits never caught him. The bank discovered his fraud only when police raided the teller'sbook and found his name on a list of heavy bettors. He had gambled embezzled money, often as much as $30,000 daily. Before the fraud ended the teller had stolen over $1.5 million.
The bank was continuously being robbed and only by chance was the thief caught.

Losses in industry are often caused through loss of inventory. Merchandise can be stolen by rendering it broken, sold, obsolete, or generating fictitious orders. In 1971, Penn Central lost 217 functional boxcars because they were classified as obsolete on computer and routed to a side railway. Fictitious orders are often typed into the computer with orders to erase any record of time or place of delivery. Grumbltled employees pose other significant problems. In one incident, a file librarian who was fired managed to mislabel all of the magnetic tapes before leaving. The company was at a standstill for days until all tapes could be read and labeled correctly. Others have left "logic bombs" in programs. A logic bomb is a set of instructions worked into an existing program which can cause anything from total destruction of files years later to the continued issuance of a terminated employee's payroll check.

The above are only isolated examples of crimes. Countless others are occurring. The problem that must be faced by computer users is why there are security breaches and how individual systems can be protected.

Why does computer crime continue?

Why are there so many security breaches? Computer security problems did not occur overnight. Computer crimes have been plaguing business management since the use of
computer systems. The first recorded crime was in 1958. Computer abuses have since increased proportionally with the increase in computer use.

The primary cause of security problems within an organization is the inactivity of management in addressing the issue. Most managers today remember totally manual information systems and, consequently, have a limited understanding of complex computer systems. Weaknesses of a paper and pencil system are more familiar than those weaknesses of rapidly changing computer systems. Control was easily maintained physically with manual systems. Today, with the downloading of information to micros at remote locations, physical security alone is not enough. Managers must now understand the needs of the larger computer system as a whole. Management will only begin to use adequate security measures if they understand the purpose and necessity of them.

Too many people trust computers because they are encased machines which appear impenetrable. Today, "money is debited and credited to accounts inside computers. In fact, the computer is rapidly becoming the vault for the business community." However, just as a bank vault has a security system, so must a computer. A government study revealed that losses from computer crimes range between $100-300 million dollars annually with an average loss of $100,000 per crime detected. "Computer use increases the dangers of large losses from the concentration of intangible assets in electronic forms and change the nature of exposure to losses with assets in these new forms." Businesses can no longer afford to
ignore the need for computer security.

However, even those companies that understand the
vulnerabilities of their systems and the necessity of security
still take no action to protect the system. Management's primary
focus is on the "bottom line." It is hard to justify the cost
of a security system. Management is eager to allocate
resources that directly increase the productivity of their
organizations. Security seldom adds directly to productivity;
it only assures protection from loss of productivity... if
security is effective it usually goes unnoticed because loss
is averted."\(^{10}\) However, if a comprehensive analysis is done
of the risk of loss without adequate security controls, it is
evident that the benefits far outweigh the cost. The only
way management will understand the benefit is by understanding
the inherent need for the security itself. Putting a dollar
value on information is difficult. A loss estimation process
should include an estimate of the business that would be
lost if files were tampered with, or possibly, the cost to
reconstruct damaged files, or the effects of losing irreplaceable
information. Secure computers do carry a price tag. When
compared to estimated losses, it is evident that the cost is
more than justified.

Another complicating factor contributing to continued
security breaches is the manner in which management chooses
tools for existing systems. Many controls are "after the
fact" remedies. If a weakness is discovered, a company over
compensates with controls in that area. An individual needs
become evident a control is installed. This piecemeal method of selecting controls is the predominant trend. However, the greatest dangers are not where losses have been anticipated, but where losses have not been anticipated. The most secure systems are those protected by a comprehensive system installed after a complete review of the entire system—not piece by piece.

In choosing controls, management must also begin to use quantitative information. Frequently, many managers use opinions of outside parties with similar needs. Quantitative, objective information is most useful. Information such as cost to install and money to be saved in the long run versus short run, or the losses to be prevented are not considered. As in any other major decision, a business must take the appropriate steps in planning and implement a security system. Implementation must be periodically followed up on to ensure protection. Periodic security reviews must also take place to ensure adequate security for changing systems. As systems are updated or modified, the entire security system must also be modified.

Apparent management ignorance contributes directly to continued security problems. Over concern for the bottom line and inadequate selection methods are causing installation of inadequate controls and, consequently, false confidence in these controls. Managers must educate themselves as to system vulnerabilities and take an increased role in detection and prevention. Managers must identify warning signals to
possible weaknesses and take appropriate corrective measures.

Sanford Sherain, a computer security specialist, has stated, "The starting point for computer security is at the top. Unless the upper most levels of management view the potential for computer loss as a problem, too little will be accomplished by those who have concern." Security must become a high priority. A successful security system requires top management involvement. Success in continued use of controls by employees is directly related to the importance management places on it. Management must take the problem seriously. Computer thieves can strike any system at any time. No system is exempt unless adequately protected.

Stopping computer crime.
Secure computer systems are an attainable goal. Management must protect systems from both internal and external threats. Each necessitates different types of controls. There are many controls companies can institute to help ensure security and deter crime. There are hardware devices such as data encryption devices which code information and can only be decoded through the use of passwords which limit access to systems. Internal policies and procedures regarding security is an effective control over users also.

Upon implementation, controls must be followed up on to ensure effectiveness and compliance by employees. Many firms have installed security systems that are disregarded or ineffectively used. Common sense alerts one that security systems be periodically checked and critically reviewed to
ensure compliance and adequacy with changing systems. A primary example of a common control that is used ineffectively is the password. A password is necessary to gain access to a system and is designed to limit access to only those with passwords. Unfortunately, easy passwords are more or less to remember terms like "password." Consequently, unauthorized users gain access by guessing. Others are so hard to remember that users find it necessary to post the password somewhere to remember it, thus losing the security. Simple standard procedures would increase security. Passwords should not be names. Passwords should be changed periodically, but not so often that they are forgotten. Each employee should have a unique password holding him individually liable. If an employee is terminated, his access code should be eliminated to avoid unauthorized use later. These simple procedural steps will help add to the effectiveness of this particular control.

One of the most beneficial steps a company can take to internal security is internal education. Software and hardware devices are helpful in deterring both external and internal thieves. However, internal thieves are most effectively stopped from within. A security department for computers should be set up or similar duties allocated to an individual high in the organization. This reflects to employees the seriousness of management to security. A policy and procedures manual should be maintained containing rules concerning use of computers, access, and security measures. If employees are
educated as to the possible security problems and methods of reporting unusual occurrences, they may be more adept in dealing with security problems and stopping them.

Computer crime is a serious problem. Losses will continue to escalate as computer use increases unless corrective measures are taken now. These crimes are the final "bug" in the transition from manual to computerized information systems. The method of dealing with security has not been worked into all systems and until then these systems are in danger of being invaded. The void in present laws only exacerbate the problem. However, "the security gap is not likely to close...until executives and computer users change their attitude toward protecting information." Users must realize the value of their information. Management especially, must identify the vulnerabilities of their system. Ignoring the problem will not make it disappear. Assuming no one would try to break into "our system" is no protection. Precautions must be taken to protect all systems. As technology and use continue to increase at such rapid rates, computer crime will also continue at an equally rapid rate. However, with the proper controls, systems can be secured and computer crime averted.


4 Pleva, p. 34.

5 Pleva, p. 32.

6 Pleva, p. 32.

7 Bureau of Justice, p. 1.

8 Bureau of Justice, p. 2.

9 Bureau of Justice, p. 2.

10 Bureau of Justice, p. 3.


12 Pleva, p. 126.
BIBLIOGRAPHY


