# THREATS TO COMPUTER SYSTEMS: AN OVERVIEW

CSL - Computer Systems Laboratory Bulletin
March 1994

Computer systems are vulnerable to many threats which can inflict various types of damage resulting in significant losses. Damage can range from minor errors which sap database integrity to fires which destroy entire computer centers. Losses can stem from the actions of supposedly trusted employees defrauding the system to outside hackers and unauthorized users roaming freely through the Internet. The exact amount of computer-related losses is unknowable; many losses are never discovered and others are covered up to avoid unfavorable publicity.

This bulletin increases reader awareness of threats to computer systems by giving a broad picture of the threat environment in which systems are operated today. An overview of many of today's common threats will be useful to organizations studying their own threat environments with a view toward developing solutions specific to their organization.

This bulletin summarizes a chapter of the computer security handbook being developed by CSL. We have already published bulletins summarizing other chapters on establishing a computer security program, considering people issues in computer security, and developing computer security policy. Additional bulletins will be issued as chapters are finalized.

### *Common Threats*

A wide variety of threats face today's computer systems and the information they process. In order to control the risks of operating an information system, managers and users must know the vulnerabilities of the system and the threats which may exploit them. Knowledge of the threat environment allows the system manager to implement the most cost-effective security measures. In some cases, managers may find it most cost-effective to simply tolerate the expected losses.

The following threats and associated losses are based on their prevalence and significance in the current computing environment and their expected growth. The list is not exhaustive; some threats may combine elements from more than one area.

### *Errors and Omissions*

Users, data entry clerks, system operators, and programmers frequently make unintentional errors which contribute to security problems, directly and indirectly. Sometimes the error is the threat, such as a data entry error or a programming error that crashes a system. In other cases, errors create vulnerabilities. Errors can occur in all phases of the system life cycle.

Programming and development errors, often called bugs, range in severity from benign to catastrophic. In the past decade, software quality has improved measurably to reduce this threat, yet software "horror stories" still abound. Installation and maintenance errors also cause security problems.

Errors and omissions are important threats to data integrity. Errors are caused not only by data entry clerks processing hundreds of transactions per day, but by all users who create and edit data. Many programs, especially those designed by users for personal computers, lack quality control measures. However, even the most sophisticated programs cannot detect all types of input errors or omissions.

The computer age saying "garbage in, gospel out" contains a large measure of truth. People often assume that the information they receive from a computer system is more accurate than it really is. Many organizations address errors and omissions in their computer security, software quality, and data quality programs.

### *Fraud and Theft*

Information technology is increasingly used to commit fraud and theft. Computer systems are exploited in numerous ways, both by automating traditional methods of fraud and by using new methods. For example, individuals may use a computer to skim small amounts of money from a large number of financial accounts, thus

generating a significant sum for their own use. Also, deposits may be intentionally misdirected. Financial systems are not the only ones subject to fraud. Systems which control access to any resource are targets, such as time and attendance systems, inventory systems, school grading systems, or long-distance telephone systems.

Fraud can be committed by insiders or outsiders. The majority of fraud uncovered on computer systems is perpetrated by insiders who are authorized users of a system. Since insiders have both access to and familiarity with the victim computer system, including what resources it controls and where the flaws are, authorized system users are in a better position to commit Crimes. An organization's former employees may also pose threats, particularly if their access is not terminated promptly.

### *Disgruntled Employees*

Disgruntled employees can create both mischief and sabotage on a computer system. Employees are the group most familiar with their employer's computers and applications, including knowing what actions might cause the most damage. Organizational downsizing in both public and private sectors has created a group of individuals with organizational knowledge who may retain potential system access. System managers can limit this threat by invalidating passwords and deleting system accounts in a timely manner. However, disgruntled current employees actually cause more damage than former employees.

Common examples of computer-related employee sabotage include:

Entering data incorrectly
Changing data
Deleting data
Destroying data or programs with logic bombs
"Crashing" systems
Holding data hostage
Destroying hardware or facilities

### *Physical and Infrastructure*

The loss of supporting infrastructure includes power failures (including outages, spikes and brownouts), loss of communications, water outages and leaks, sewer problems, lack of transportation services, fire, flood, civil unrest, strikes, and so forth. These losses include dramatic events such as the explosion at the World Trade Center and the Chicago tunnel flood as well as more common events such as a broken water pipe. System owners must realize that more loss is associated with fires and floods than with viruses and other more widely publicized threats.

A loss of infrastructure often results in system downtime, sometimes in unexpected ways. For example, employees may not be able to get to work during a winter storm, although the computer system may be functional.

### *Malicious Hackers*

Hackers, sometimes called crackers, are a real and present danger to most organizational computer systems linked by networks. From outside the organization, sometimes from another continent, hackers break into computer systems and compromise the privacy and integrity of data before the unauthorized access is even detected. Although insiders cause more damage than hackers, the hacker problem remains serious and widespread.

The effect of hacker activity on the public switched telephone network has been studied in depth. Studies by the National Research Council and the National Security Telecommunications Advisory Committee show that hacker activity is not limited to toll fraud. It also includes the ability to break into telecommunications systems (such as switches) resulting in the degradation or disruption of system availability. While unable to reach a conclusion about the degree of threat or risk, these studies underscore the ability of hackers to cause serious damage.

The hacker threat often receives more attention than more common and dangerous threats. The U.S. Department of Justice's Computer Crime Unit suggests three reasons. First, the hacker threat is a more recently encountered threat. Organizations have always had to worry about the actions of their own employees and could use disciplinary measures to reduce that threat. However, these controls are ineffective against outsiders who are not subject to the rules and regulations of the employer.

Secondly, organizations do not know the purposes of a hacker; some hackers only browse, some steal, some damage. This inability to identify purposes can suggest that hacker attacks have no limitations. Finally, hacker attacks make people feel vulnerable because the perpetrators are unknown.

### *Industrial Espionage*

Industrial espionage involves collecting proprietary data from private corporations or government agencies for the benefit of another company or organization. Industrial espionage can be perpetrated either by companies seeking to improve their competitive advantage or by governments seeking to aid their domestic industries. Foreign industrial espionage carried out by a government is known as economic espionage.

Industrial espionage is on the rise. The most damaging types of stolen information include manufacturing and product development information. Other types of information stolen include sales and cost data, client lists, and research and planning information.

Within the area of economic espionage, the Central Intelligence Agency states that the main objective is obtaining information related to technology, but that information on U.S. government policy deliberations concerning foreign affairs and information on commodities, interest rates, and other economic factors is also a target. The Federal Bureau of Investigation concurs that technology-related information is the main target, but also cites corporate proprietary information such as negotiating positions and other contracting data as a target.

### *Malicious Code*

Malicious code refers to viruses, worms, Trojan horses, logic bombs, and other "uninvited" software. Malicious code is sometimes mistakenly associated only with personal computers, but can also attack more sophisticated systems. However, actual costs attributed to the presence of malicious code have resulted primarily from system outages and staff time involved in repairing the systems. Nonetheless, these costs can be significant.

### *Malicious Software: A Few Key Terms*

Virus: A code segment which replicates by attaching copies of itself to existing executables. The new copy of the virus is executed when a user executes the new host program. The virus may include an additional "payload" that triggers when specific conditions are met. For example, some viruses display a text string on a particular date. There are many types of viruses including variants, overwriting, resident, stealth, and polymorphic.

Trojan Horse: A program that performs a desired task, but also includes unexpected (and undesirable) functions. Consider as an example an editing program for a multi-user system. This program could be modified to randomly delete one of the users' files each time they perform a useful function (editing) but the deletions are unexpected and definitely undesired!

Worm: A self-replicating program which is self-contained and does not require a host program. The program creates a copy of itself and causes it to execute; no user intervention is required. Worms commonly utilize network services to propagate to other host systems.

The number of known viruses is increasing, and the rate of virus incidents is growing moderately. Most organizations use anti-virus software and other protective measures to limit the risk of virus infection.

### *Foreign Government Espionage*

In some instances, threats posed by foreign government intelligence services may be present. In addition to possible economic espionage, foreign intelligence services may target unclassified systems to further their intelligence missions.

### *Threats to Personal Privacy*

The accumulation of vast amounts of electronic information about individuals by the government, credit bureaus, and private companies combined with the ability of computers to monitor, process, aggregate, and record information about individuals have created a very real threat to individual privacy. The possibility that all of this

information and technology could be linked together has loomed as a specter of the modern information age. This phenomenon is known as "big brother."

The threat to personal privacy arises from many sources. Several cases have been reported involving the sale of personal information by federal and state employees to private investigators or other "information brokers." One such case was uncovered in 1992 when the Justice Department announced the arrest of over two dozen individuals engaged in buying and selling information from Social Security Administration (SSA) computer files. In the course of the investigation, auditors learned that SSA employees had unrestricted access to over 130 million employment records.

Just recently, an investigation found that five percent of the employees in one region of the Internal Revenue Service had browsed through tax records of friends, relatives, and celebrities. Some employees used the information to create fraudulent tax refunds, but many acted simply out of curiosity.

As more of these cases come to light, many individuals express increased concern about threats to their personal privacy. Over the years, Congress has enacted legislation, such as the Privacy Act of 1974 and the Computer Matching and Privacy Protection Act of 1988, which defines the boundaries of the legitimate uses of personal information collected by the government.

While the magnitude and cost to society of the personal privacy threat are difficult to gauge, information technology has become powerful enough to warrant fears of both government and corporate "big brothers." Increased awareness of the problem is needed.

### *Conclusion*

Today's computer systems, linked by national and global networks, face a variety of threats which can result in significant financial and information losses. Threats vary considerably, from threats to data integrity resulting from unintentional errors and omissions to threats to system availability from malicious hackers attempting to crash a system. An understanding of the types of threats in today's computing environment can assist a security manager in selecting appropriate cost-effective controls to protect valuable information resources.