National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

An Introduction to Computer Security: The NIST Handbook

- D R A F T -

June 20, 1994

Table of Contents

Part I
Introduction & Overview

Part II
Management Controls

Part III
Operational Controls

Part IV
Technical Controls

Part V
Example

Part I
Introduction & Overview

1 Introduction

1.1 Purpose

The purpose of this Handbook is to assist managers in securing computer-based resources (including hardware, software, and information) by explaining important concepts, cost considerations, and interrelationships of security controls. Such knowledge is vital for managers to make informed decisions in selecting cost-effective, appropriate controls to protect systems in their unique operating and threat environments.

The Handbook provides a broad overview of the field of computer security. It assists the reader understand of their computer security needs and to develop a sound approach to the selection of appropriate security controls. The document does not, however, describe detailed steps necessary to implement a computer security program, provide detailed implementation procedures for security controls, or give guidance for auditing the security of specific systems. References of how-to books and articles that give further information are also provided.

1.2 Intended Audience

The Handbook targets federal employees[1] who have computer security responsibilities, but need assistance understanding computer security concepts and techniques. The concepts presented in the Handbook are, for the most part, applicable to the private sector, as well, as are the cost considerations and interdependencies. While there are many differences between federal and private sector computing, especially in terms of priorities and legal constraints, the underlying principles of computer security and the available safeguards -- managerial, operational, and technical -- are the same.

The Handbook is most useful to anyone who needs to learn the basics of computer security or wants a broad overview of the subject. The document is, however, probably too detailed to be employed as a user awareness guide and not sufficiently detailed to guide actual specific implementation in specific systems.[2]

1.3 Organization

I. The *Introduction & Overview* section contains three chapters:

- Handbook Introduction

---

[1] Congress assigned responsibility to NIST in the Computer Security Act of 1987 for the preparation of standards and guidelines for the security of *federal* unclassified systems.

[2] References are provided for guidance on implementation specifics.

- Approach to Security
- Roles and Responsibilities
- Threats: A Brief Overview

The Approach to Security chapter explains the underlying assumptions of computer security that are used throughout the Handbook. For example, one important assumption that is repeatedly stressed is that only security measures that are cost-effective should be implemented. A familiarity with the assumptions is fundamental to understanding the Handbook's philosophical approach to the issue of security. Following presentation of these assumptions, a discussion of the roles and responsibilities of those involved in security computer systems is presented. The threat chapter which provides the reader with an overview of the types of threats that may exist in their computing environment.

The next three sections: 1) Management Controls[3], 2) Operational Controls, and 3) Technical Controls, provide the reader with information about specific controls. The categorization into three areas was done to assist to the reader in locating information on specific areas or topics. Most controls cross the boundaries between management, operational, and technical. Each chapter in the three sections provides a basic explanation of the control; some cost considerations in selecting, implementing, and using the control; and some important interdependencies that may exist with other controls. Each chapter also provides references that may be useful in actual implementation.

II. The *Management Controls* section addresses security topics that can be characterized as managerial. They are techniques and concerns that must be addressed by management in the organization's computer security program. In general, they focus on the management of the computer security program and the management of risk within the organization. The areas discussed here are not, in general, specific to a particular system -- as is seen with operational and technical controls. This section presents:

- Computer and Information Security Policy
- Security Program Management and Administration
- Security in the System Life Cycle
- Risk Management
- Assurance

III. The *Operational Controls* section addresses security controls that focus on controls that are, broadly speaking, implemented and executed by people. These controls are

[3] The term management controls is used in a broad sense and encompasses areas that do not fit neatly into operational or technical controls.

put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise -- and can be highly interdependent with management activities as well as technical controls. Chapters presented here are:

- Personnel/User Issues
- Contingency Planning
- Computer Security Incident Handling
- Awareness and Training
- Computer Support and Operations
- Physical and Environmental Protection

IV. The *Technical Controls* section focuses on security controls that are executed by the system. These controls are dependent upon the proper functioning of the system for their effectiveness. The implementation of technical controls, however, always requires significant operational considerations -- and must be consistent with the management of security within the organization. Chapters included are:

- Identification and Authentication
- Access Control
- Audit
- Cryptography

V. The *Example* section describes a description of a hypothetical system and discusses some of the controls which have been implemented to protect the system. This section helps the reader better understand the decisions that must be made in securing a system, and illustrates the interrelationships among controls.

1.4 Computer Security's Legal Foundation

Although the Handbook does not address the legal requirements for protecting systems and information, readers should become familiar with applicable laws and regulations.

A number of laws and regulations mandate protection of federal computer and related resources. These authorities establish classes of protected data (e.g., personal data) and formalize sound computer security management practices within the federal government. The most important are listed below.

- The *Computer Security Act of 1987* requires agencies to conduct computer security training and develop computer security plans.

- The *Privacy Act of 1974* requires the protection of personal information and restricts its use to the purpose for which it was collected.

- The *Federal Managers' Financial Integrity Act* requires that financial systems use internal controls. (See also OMB Circular A-127.)

- The *Paperwork Reduction Act* and its reauthorization of 1986, updates the administration and management of computer resources.

- *OMB Circular A-123* specifies policies and standards for the establishment and maintenance of internal control programs in federal agencies.

- *OMB Circular A-127* specifies policies and standards for the establishment and maintenance of controls for financial management systems.

- *OMB Circular A-130* (specifically Appendix III) requires that federal agencies establish security programs containing specified elements.

- The *Federal Information Resources Management Regulation* (FIRMR) is the primary regulation for the use, management and acquisition of computer resources in the federal government.

- The *Brooks Act*, as amended, assigns responsibilities to the General Services Administration, Department of Commerce, and the Office of Management and Budget for the management computer resources in the federal government.

- The *Freedom of Information Act* requires that federal information be made available to the public except under certain specified conditions.

Definition of Sensitive Information

Many people think that sensitive information only requires protection from unauthorized disclosure. However, the Computer Security Act provides a much broader definition of the term "sensitive" information:

any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

The above definition can be contrasted with the long-standing confidentiality-based information classification system for national security information (i.e., CONFIDENTIAL, SECRET, and TOP SECRET). This system is based only upon the need to protect classified information from unauthorized disclosure; the U.S. Government does not have a similar governmentwide system for unclassified information. No governmentwide schemes exist which are based on the need to protect the integrity or availability of information.

Federal managers are responsible for familiarity and compliance with applicable legal requirements. However, laws and regulations, do not normally provide detailed instructions for protecting computer-related assets. Instead, they specify requirements -- such as restricting the availability of personal data to authorized users. This Handbook aids the reader in developing an effective, overall security approach and in selecting cost-effective controls to meet such requirements.

2 Approach to Security

2.1 Introduction

> *Computer security* is the protection of the integrity, availability and, if needed, confidentiality of automated information and the resources used to enter, store, process, and communicate it.

This chapter describes six basic underlying assumptions of computer security taken in this Handbook. Familiarity with these assumptions will aid the reader in better understanding how the security controls (discussed in later sections) support the overall security program goals.

2.2 What is Computer Security?

There are many different ways of looking at computer security. Some people see computer security as a way to prevent future losses; some regard it as a way to manage technology-related risks; some consider it a necessary evil to keep malicious people from harming systems; and others recognize it as a form of quality assurance. Despite these different perceptions, a common definition of computer security is still possible. Computer security is the protection of the integrity, availability and, if needed, confidentiality of automated information and the resources used to enter, store, process, and communicate it.

This chapter describes six basic underlying assumptions of computer security taken in this Handbook. Familiarity with these assumptions will aid the reader in better understanding how the security controls (discussed in later sections) support the overall security program goals.

2.3 Specific Assumptions

The six philosophical assumptions about computer security which form the foundation for this Handbook are presented in this section. Briefly, computer security:

1) supports the mission of the organization;

2) helps manage risk;

3) is an integral responsibility of sound management;

4) must be specifically assigned;

5) requires a comprehensive approach; and

6) should be cost-effective.

Assumption #1: Computer security supports the mission of the organization.

The purpose of computer security is to protect valuable organization resources such as information, hardware, and software. By providing such protection, security helps protect organization physical and financial resources, reputation, legal position, employees, and other assets. Unfortunately, security is sometimes viewed as thwarting the mission of the organization by imposing bothersome rules and procedures on users. Security rules and procedures should not exist for their own sake -- they should support the overall organization mission by protecting its assets.

Assumption #2: Computer security helps manage risk.

Managers are faced with risks which arise from the organization's use of computers which are vulnerable to a wide range of threats. (See the Threat chapter.) Computer security helps an organization analyze threats and vulnerabilities and take appropriate steps to reduce or manage the associated risks in a cost-effective manner.

While computer security helps to manage risk, it does *not* eliminate it. In addition, the exact level of risk can never be known since there is always some degree of uncertainty. Ultimately, management must decide upon the level of risk it is willing to accept. Judging what level can be tolerated, particularly when weighed against the costs of security controls, can be a difficult management decision. Management's responsibilities in this area are seen as so important that, in the federal government, there is a formal process for management acceptance of a given level risk. It is referred to as *accreditation*. When accrediting a system, the responsible official explicitly accepts the risks associated with its operation. (See the Risk Management and Life Cycle chapters.)

Assumption #3: Computer security is an integral responsibility of sound management.

One of management's responsibilities in any organization is to manage the risks (as is reasonably practicable) that can threaten the organization. Computer security helps management do this. Similar to managing other critical organization resources such as time, money, and employees, is the responsibility to manage information and associated computer assets. Information is often as critical as other assets because organizations depend on it to meet their missions. Information must be available, accurate, and complete. In some cases, access to certain information must also be restricted.

Management at the department or agency level usually exercises its responsibilities for computer security and the protection of organizational assets by taking the very important step of establishing a computer security program, usually through the issuance of *policy*. Policies documents management's decisions to expend resources to establish and implement a program and also describes how the organization will approach security. This process entails setting priorities, establishing programs, and assigning responsibilities. (The Policy chapter discusses various types of policy.)

Assumption #4: Computer security responsibilities must be specifically assigned.

To ensure that management's wishes with respect to computer security actually get implemented, responsibilities must be assigned. This process assures *accountability*. Management uses *policy* to formally assign security responsibilities to specific offices or individuals within the organization.[4] Groups or organizations which are typically assigned computer security responsibilities include: security managers, functional managers, system operators, application managers, the physical security officer, the disaster recover office, users, and the audit office.[5]

Assumption #5: Computer security requires a comprehensive approach.

Providing effective computer security requires a comprehensive approach which considers a variety of areas both within and outside of computer security. The effectiveness of security controls requires that other controls and management disciplines work together. The reader should be aware that many other activities, even those not directly related to security, can negate, reduce, or sometimes even enhance the effectiveness of security controls.

Interdependencies of Security Controls

> A security architecture or program is comprised of several building blocks, which are referred to as *security controls*. These controls are divided in this Handbook into three groups: managerial, operational, and technical controls.

Security controls often depend upon the proper functioning of other controls to work effectively -- in fact, many such interdependencies exist.[6] If appropriately chosen, managerial, operational, and technical controls can work together synergistically. On the other hand, without a firm understanding of the interdependencies of security controls, they can actually undermine one another. For example, without proper training on how and when to use a virus detection package, the user may utilize the package incorrectly and therefore ineffectively. As a result, the user may mistakenly believe that their system will always be virus-free. In reality, these interdependencies are usually more complicated and difficult to ascertain.

Other Interdependencies

The effectiveness of security controls also depends on factors such as system management, legal issues, quality assurance, and internal and management controls. Computer security must also work with traditional security disciplines including physical and personnel security. Many other important interdependencies exist which are often unique to the organization or system environment. Managers must recognize how computer security relates to other areas

[4] Policy also has other uses, as described in the Policy chapter.

[5] This list is not intended to be all-inclusive; indeed, since organizations vary so considerably, no list could be.

[6] Each of the chapters describing a control includes a section on "interdependencies," to reinforce this point.

of systems and organizational management.

Assumption #6: Safeguards must be cost-effective.

The final assumption of computer security is that security safeguards must be cost-effective. The costs and benefits of security must be carefully examined to ensure that the cost of controls does not exceed expected benefits. Recognize that costs and benefits must be judged in both monetary and non-monetary terms.[7]

Security is a smart business practice. By investing in security measures, an organization can reduce the frequency and severity of computer security-related losses. For example, an organization estimates that it is experiencing significant losses per year in inventory through fraudulent manipulation of the computer system. Security measures, such as an improved access control system, may be able to significantly reduce the loss.

The benefits of security are not only monetary. A sound security program can thwart hackers and can reduce the frequency of viruses. Elimination of these kinds of threats can reduce unfavorable publicity as well as increase morale and productivity.

Security benefits, however, do have both direct and indirect costs. Direct costs include purchasing, installing, and administering security measures, such as access control software or fire suppression systems. Additionally, security measures can sometimes affect system performance, employee morale, or retraining requirements. All of these must be considered in addition to the basic cost of the control itself. In many cases, these additional costs may well exceed the cost of the base control (as is often seen, for example. in the costs of administering a supplementary access control package). Solutions to security problems that cost more, directly or indirectly, than simply tolerating the problem are not cost-effective.

2.4 Summary

The assumptions presented in this chapter provide a basic structure for managers to address computer security issues. With a solid grasp of the underlying approach that this Handbook takes toward computer security, readers are better able to take advantage of the basic concepts, cost considerations, and interdependencies of security controls.

---

[7] A section on "cost consideration" is included in the each of the security control chapters which follow.

3 Roles & Responsibilities

3.1 Introduction

One fundamental issue that arises in discussions of computer security is: **"Whose responsibility is it?"** Ultimately, of course, the answer is a simple one: security is the responsibility of everyone who interacts in some way with a computer system. There are, however, significant variations in the specific duties and responsibilities of individuals and organizational entities with respect to computer security.

> Many offices and individuals have responsibilities for computer security.

This chapter presents a brief overview of roles and responsibilities of the various officials and organizational offices *typically* involved with computer security.[8] This chapter is intended to give the reader a basic familiarity with the major officials and organizational elements that play a role in computer security. *It does not describe all responsibilities of each in detail, nor will this chapter apply uniformly to all organizations.* Organizations, like individuals, have unique characteristics and no single template can apply to all. As with the rest of the Handbook, *this chapter is not intended to be used as an audit guide*.

Individuals and organizations in this section are categorized into the following groups:

- executives / senior management
- program/functional managers/application owners,
- computer security management,
- technology providers,
- supporting organizations, and
- users.[9]

Executives are responsible for establishing an organization's computer security program and

---

[8] Note that this includes groups *within* the organization; outside organizations (e.g., NIST and OMB) are not included in this chapter.

[9] Note that these categories are generalizations and are used to help aid the reader; if they are not applicable to the reader's particular system, they can be safely ignored. Also, some organizations (e.g., the Personnel Office) may fall into more than one category.

policies and providing the resources and support for the program. Program and functional managers/application owners are those who are supported by technology and who have responsibility for managing information systems. Computer security management includes those directly involved in establishing and operating the computer security program. The technology providers category involves those who support the organization by providing technology services (e.g., the maintenance of a LAN). Supporting organizations includes those organizational elements which provide significant services to the computer security program (e.g., the office which handles personnel background screening), but are not directly responsible for overall computer security program operations. Finally, are users who directly or indirectly work with the computer system.

3.2 Executives / Senior Management

> Senior management has ultimate responsibility for the security of their organization's computer systems.

Executives are those senior managers who are ultimately responsible for the success of the organization and how computer security supports its mission. They establish the organization's computer security program (usually through the issuance of policy) and its overall program goals, objectives, and priorities. They are responsible for ensuring that adequate resources are applied to the program and are also responsible, ultimately, for the success of the program.

3.3 Program and Functional Managers / Application Owners

Functional Manager/Application Owner: This is the person who is responsible for the system or the manager of a function that the system was created to serve. This is also normally the *accrediting official* (as discussed in the life cycle chapter) who approves their system to operate. The Functional Manager/Application Owner has responsibility for their system, including its security and the management, operational, and technical controls. This person has responsibility for approving who is granted access to their applications.

The Functional Manager/Application Owner usually is assisted by a technical staff that oversees the actual workings of the system. This kind of support is no different for other staff members who work on other program implementation issues.

Functional Manager's Security Officer. This person assists the Functional Manager/ Application owner in the development of security requirements and in seeing that they are implemented.

3.4 Computer Security Management

The *Computer Security Program Manager* (and their support staff) directs the organization's day-to-day management of the organization's computer security program. This individual is responsible for ensuring the effective interaction of the disparate organizational elements involved in the computer security program -- including those external to the organization.

System Security Manager/Officers, although not normally part of the computer security program management office, are responsible for coordinating the security efforts of particular systems. This person works closely with the *Functional Manager's Security Officer* and senior management.

> **What is a program/functional manager?**
>
> The term *program/functional manager* or *application owner* may not be familiar or immediately apparent to all readers. The examples provided below should help the reader better understand this important designation. In reviewing these examples, note that computer systems often serve more than one group or function.
>
> *Example #1*. A personnel system serves an entire organization, however, the Personnel Manager would normally be the application owner. This applies even if the application is distributed so that supervisors and clerks throughout the organization use and update the system.
>
> *Example #2*. A Federal benefits systems provides benefit checks to 500,000 citizens on a monthly basis. The processing is done on a mainframe data center. The Benefits Program Manager is the application owner.
>
> *Example #3*. A mainframe data processing organization supports several large applications. The mainframe director is *not* the functional manager for any of the applications.
>
> *Example #4*. A 100-person division has a diverse collection of personal computers, UNIX workstations, and minicomputers used for general office support, Internet connectivity, and computer-oriented research. The division director would normally be the Functional Manager responsible for the system.

3.5 Technology Providers

System Management/System Administrators are the management and technical staff that program, operate, and troubleshoot computer systems. System management is generally used to refer to large systems, with a staff of people. System administrators is often used to refer to smaller systems with only one or two technical staff. They are responsible for implementing technical security on computer systems and for being familiar with security technology that relates to their system. They also must ensure the continuity of their services to meet the needs of functional managers as well as analyzing technical vulnerabilities in their systems (and their security implications). Often assisting system management officials in this effort is a *system security manager/officer* (as discussed in the preceding section) responsible for day-to-day security administration duties. The power of the system administrator is a major issue in securing systems.

Help Desk. Whether or not a Help Desk is tasked with incident handling or not, they must be able to recognize security incidents and refer the caller to the appropriate person or organization for a response.

Communications/Telecommunications Staff. This office is normally responsible for the provision of communications services, including voice, data, video, and fax service. They have similar responsibilities for communications systems as systems management officials have for their systems. It is also important that they be knowledgeable in the use of cryptography to protect data as it crosses their networks (as appropriate).

3.6 Supporting Functions

Auditors. Auditors are responsible for examining systems to see whether the system is meeting stated security requirements including system and organization policies and whether security controls are appropriate. Audits can be performed by those operating the system under review or by outside auditors (who should have no professional links to the correct operation of the system).

Physical Security. The physical security office is responsible for developing and enforcing appropriate physical security controls, in consultation with computer security management, program and functional managers, and others as appropriate. Physical security is addressed not only central computer installations, but office environments as well.

Disaster Recovery/Contingency Planning Staff. Some organizations have a separate disaster recovery/contingency planning staff. In this case, they are normally responsible for contingency planning for the organization as a whole and normally work with functional mangers/application owners and others to obtain additional Contingency Planning support, as needed.

Quality. Many organizations have established a quality assurance program to improve the products and services they provide to their customers. The quality officer should have a working knowledge of computer security and how it can be used to improve the quality program by, for example, improving the integrity of computer-based information, the availability of services, and the confidentiality of customer information as appropriate. In turn, quality is important in the computer security program as discussed in the assurance chapter.

> The supporting organizations discussed in the text are often also users of systems and may include many functional managers/application owners.

Procurement. The procurement office is responsible for ensuring that organizational procurements have been reviewed by appropriate officials. The procurement office cannot be responsible for ensuring that goods and services meet computer security expectations, because they lack the technical expertise. This office should, however, be expected to be knowledgeable about computer security standards and for bringing them to the attention of those requesting such technology.

Training Office. An organization must decide whether the primary responsibility for training users, operators, and managers in computer security rests with the Training Office or the Computer Security Program Office. In either case, the two organizations should work together to develop an effective training program.

Personnel. The personnel office is normally the first point of contact in helping managers determine if a security background investigation is necessary for a particular position (in conjunction with the security office). The personnel office may also be responsible for providing security related personnel exit procedures when employees leave an organization (e.g., by transfer, retirement, or reassignment).

Risk Management/Planning Staff. Many organizations have a full-time staff devoted to studying all types of risks to which the organization may be exposed. This function may include computer-security related risks, although this office may not actually perform risk analyses of specific computer systems.

Physical Plant. This office is responsible for ensuring the provision of such services as electrical power and environmental controls, necessary for the safe and secure operation of an organization's systems. Often they are augmented by separate medical, fire, hazardous waste, or life safety personnel.

3.7 Users

Users of Information. There are many types of users of information. Some people use the system directly, others read reports, and others input information into their systems. Some users of information may be very far removed from the computer system. Users of information are responsible for letting the Functional Manger/Application Owner (or their representative) know what their needs are for the protection of the information.

Operators of Systems/Users. Operators are responsible for following security procedures, for reporting security problems, and for attending required computer security and functional training.

3.8 Summary

The various officials and organizational elements discussed in this chapter play varying but important roles in supporting the organization's overall computer security program. The support and cooperation from all personnel is an essential key to a successful computer security program.

4 Threats: A Brief Overview

4.1 Introduction

Often managers are first confronted with computer security issues when they are asked to expend resources to protect a system. They naturally ask themselves why they should do so. The reason is simple. Computer systems are vulnerable to many threats -- which can inflict various types of damage resulting in significant losses. This damage can range from minor errors which sap database integrity to fires which can destroy entire computer centers. Losses can stem from the actions of supposedly trusted employees defrauding the system to outside hackers roaming uncontained through the Internet. The exact amount of computer-related losses is unknowable since many losses are never discovered and others are "swept under the carpet" to avoid unfavorable publicity. Other kinds of threats also arise from the use of computers, such as those to personal privacy.

The purpose of this chapter is to give the reader a broad sense of the threat environment in which systems are operated today; it is not intended to be a methodical documentation of each and every kind of threat to every system in every environment.[10] This overview of many of today's common threats may prove useful to organizations studying their own threat environments; however, the perspective of this chapter is very broad. Threats against any particular systems could be quite different from those discussed here.

4.2 Common Threats

A wide variety of threats face today's computer systems and the information they process. Knowledge of the types of threats and vulnerabilities aids in the application of the most cost-effective security measures (with the realization that, in some cases, it may be more cost-effective to simply tolerate the expected losses). In order to manage the risks of operating an information system, knowledge of threats (and the vulnerabilities they may exploit) is necessary. Analysis of an system's specific threats usually takes place when conducting a risk analysis. (See the Risk Management chapter.)

The threats and associated losses presented below were selected based on their prevalence and significance in the current computing environment and their expected growth. This list is not exhaustive, and some threats may combine elements from more than one area.

4.2.1 Errors and Omissions

Users, data entry clerks, system operators, and programmers frequently make unintentional errors which contribute directly and indirectly to security problems. In some cases, the error

[10] This chapter also is not intended to address threats to national security systems.

is the threat, such as a data entry error or a programming error that crashes a system. In other cases, the errors create vulnerabilities. Errors can occur during all phases of the system life cycle. A long-term survey of computer-related economic losses conducted by Robert Courtney, a computer security consultant and former member of the Computer System Security and Privacy Advisory Board, found that 65 percent of losses to organizations were the result of errors and omissions.[11]

Programming and development errors, often called bugs, can range in severity from benign to catastrophic. In a 1989 study for the House Committee on Science, Space and Technology, entitled *Bugs in the Program,* the staff of the Subcommittee on Investigations and Oversight summarized the scope and severity of this problem in terms of government systems as follows:

> As expenditures grow, so do concerns about the reliability, cost and accuracy of ever-larger and more complex software systems. These concerns are heightened as computers perform more critical tasks, where mistakes can cause financial turmoil, accidents, or in extreme cases, death.[12]

Since that time, the software industry has changed considerably, with measurable improvements in software quality. Yet software "horror stories" still abound, and the basic principles and problems analyzed in the report remain the same.

Installation and maintenance errors are another source of security problems. For example, an audit by the President's Council for Integrity and Efficiency (PCIE) in 1988 found that every one of the ten mainframe computer sites studied had installation and maintenance errors that introduced significant security vulnerabilities.[13]

Errors and omissions are an important threat to data integrity. These errors are caused not only by data entry clerks processing hundreds of transactions per day, but by all types of 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,

---

[11] Robert Courtney Survey of Computer Security: 1988-1991, cited in Computer System Security and Privacy Advisory Board, *1991 Annual Report,* March 1992, 18.

[12] House Committee on Science, Space and Technology, Subcommittee on Investigations and Oversight, *Bugs in the Program: Problems in Federal Government Computer Software Development and Regulation,* 101st Cong., 1st sess., 3 August 1989, 2.

[13] Review of General Controls in Federal Computer Systems, President's Council on Integrity and Efficiency, October, 1988.

software quality, and data quality programs.

4.2.2 Fraud and Theft

The growth of information technology has led to increased threats that the technology will be used to commit fraud and theft. One study found that in 1992, $882 million worth of personal computers were lost due to theft.[14] Computer systems can be exploited for these purposes, in numerous ways, both by "automating" traditional methods of fraud and 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, e.g., time and attendance systems, inventory systems, school grading systems, or long-distance telephone systems.

These types of activities can be committed by insiders or outsiders. The majority of fraud uncovered on computer systems is perpetrated by insiders (i.e., authorized users of a system). A 1993 *InformationWeek*/Ernst and Young study found that 90 percent of Chief Information Officers viewed employees "who do not need to know" information as threats.[15] The U.S. Department of Justice Computer Crime Unit states that "insiders constitute the greatest threat to computer systems."[16] 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 with their knowledge of an organization's operations may also pose threats, particularly if their access is not terminated promptly. (See below.)

The threat from outsiders is discussed below in the section on hackers.

4.2.3 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. The downsizing of organizations in both the public and private sectors has created a group of individuals with organizational knowledge, who may retain potential system access (e.g., if system accounts

---

[14] "Reporting Computer Losses," *USA Today*, April 21, 1993.

[15] Bob Violino and Joseph C. Panettieri, "Tempting Fate," *InformationWeek*, October 4, 1993: 42.

[16] Letter from Scott Charney, Chief, Computer Crime Unit, U.S. Department of Justice, to Barbara Guttman. July 29, 1993.

are not deleted in a timely manner).[17]

Common examples of computer-related employee sabotage include:

- Destroying hardware or facilities
- Planting logic bombs that destroy programs or data[18]
- Entering data incorrectly
- "Crashing" systems
- Deleting data
- Holding data hostage
- Changing data

Martin Sprouse, author of *Sabotage in the American Workplace,* reported that the motivation for sabotage can range from altruism to revenge:

> As long as people feel cheated, bored, harassed, endangered, or betrayed at work, sabotage will be used as a direct method of achieving job satisfaction -- the kind that never has to get the bosses' approval.[19]

4.2.4 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. Many of these issues are covered in the Chapter on Physical and Environmental Controls. It may take considerable effort to convince system owners that much more loss is associated with fires and floods than with viruses and other more widely publicized threats.

The Courtney study found that 8 percent of losses resulted from infrastructure failures (such as power outages, fires, floods) and 5 percent were attributable to water damage.[20] (The latter figure does not include floods and water damage from fire suppression.) 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.

---

[17] Charney

[18] E.g., to be activated if an employee's name is removed from the personnel list.

[19] Martin Sprouse, ed., *Sabotage in the American Workplace: Anecdotes of Dissatisfaction, Mischief and Revenge* (San Francisco: Pressure Drop Press, 1992), 7.

[20] Courtney, 18.

4.2.5 Malicious Hackers

Hackers, sometimes called crackers, are the current "bogeymen" of computer security. One 1992 study of a particular Internet site (i.e., one computer system) found that hackers attempted to break in once at least every other day.[21] The hacker threat must be considered in terms of past and potential future damage. Although current losses due to hacker attacks are significantly smaller than losses due to insiders[22] (see sections on fraud and industrial espionage), the hacker problem is widespread and serious.

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.[23] [24]

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 for this. 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. Third, hacker attacks make people feel vulnerable, because they are unknown. For example, suppose a painter is hired to paint a house and, once inside, steals a piece of jewelry. Other homeowners in the neighborhood will not feel threatened by this crime and will protect themselves by not doing business with that painter. But if a burglar breaks into the same house and steals the same piece of jewelry, the entire neighborhood may feel victimized and vulnerable.[25]

---

[21] Steven M. Bellovin, "There Be Dragons" Proceedings of the Third Usenix UNIX Security Symposium.

[22] While insiders can also "hack" computer systems, the term "hackers" is used in this case to refer exclusively to outsiders.

[23] National Research Council, *Growing Vulnerability of the Public Switched Networks: Implication for National Security Emergency Preparedness,* (Washington, DC: National Academy Press, 1989).

[24] Report of the National Security Task Force, November 1990.

[25] Charney.

4.2.6 Industrial Espionage

Industrial espionage is the act of gathering proprietary data from private companies or the government[26] for the purpose of aiding another company(ies). 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 often referred to as economic espionage.

Industrial espionage is on the rise. A 1992 study sponsored by the American Society for Industrial Security (ASIS) found that proprietary business information theft had increased 260 percent since 1985. The data indicated that 30 percent of the reported losses in 1991 and 1992 had foreign involvement. The study also found that 58 percent of thefts were perpetrated by current or former employees. (Note: The figures of 30 and 58 percent are not mutually exclusive.) The three most damaging types of stolen information were pricing information, manufacturing process information, and product development and specification information. Other types of information stolen included customer lists, basic research, sales data, personnel data, compensation data, cost data, proposals, and strategic plans.[27]

Within the area of economic espionage, the Central Intelligence Agency (CIA) has stated 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.[28] The Federal Bureau of Investigation concurs that technology-related information is the main target, but also lists corporate proprietary information such as negotiating positions and other contracting data as a target.[29]

4.2.7 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.

---

[26] The government is included here because it often is the custodian for proprietary data (e.g., patent applications).

[27] Richard J. Heffernan and Dan T. Swartwood, "Trends in Competitive Intelligence," *Security Management* 37, no. 1 (January 1993): 70-73.

[28] Robert M. Gates, testimony before the House Subcommittee on Economic and Commercial Law, Committee on the Judiciary, 29 April 1992.

[29] William S. Sessions, testimony before the House Subcommittee on Economic and Commercial Law, Committee on the Judiciary, 29 April 1992.

A 1993 study of viruses found that while the number of known viruses is increasing exponentially, the number of virus incidents is not.[30] The study concluded that viruses are becoming more prevalent, but only "gradually."

> The rate of PC-DOS virus incidents in medium to large North American businesses appears to be approximately 1 per 1000 PCs per quarter; the number of infected machines is perhaps 3 or 4 times this figure if we assume that most such businesses are at least weakly protected against viruses.[31]

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.

Source: NIST Special Publication 800-5.

4.2.8 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.

4.2.9 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 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 has been referred to as "big brother."

The threat to personal privacy arises from many sources. There have been several cases where the sale of personal information by federal and state employees was made to private

---

[30] Jeffrey O. Kephart and Steve R. White, "Measuring and Modeling Computer Virus Prevalence," Proceedings, 1993 IEEE Compute*r Society Symposium on Research in Security and Privacy* (May 1993): 14.

[31] ibid.

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.[32] 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 5 percent of the employees in one region of the IRS had browsed through tax records of friends, relatives, and celebrities.[33] Some of the employees used the information to create fraudulent tax refunds, but many were acting simply out of curiosity.

As more of these cases come to light, many individuals are becoming increasingly concerned about threats to their personal privacy. A July 1993 special report in *MacWorld* cited polling data taken by Louis Harris and Associates showing that in 1970 only 33 percent of respondents were concerned about personal privacy. By 1990, that number had jumped to 79 percent.[34]

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, it is apparent that information technology is becoming powerful enough to warrant fears of both government and corporate "big brothers." Increased awareness of the problem is needed.

4.3 Summary

A wide variety of threats face computer systems 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 particular types of threats can aid a security manager in selecting appropriate cost-effective controls to protect their systems and information.

---

[32] House Committee on Ways and Means, Subcommittee on Social Security, *Illegal Disclosure of Social Security Earnings Information by Employees of the Social Security Administration and the Department of Health and Human Services' Office of Inspector General: Hearing,* 102nd Cong., 2nd sess., 24 September 1992, Serial 102-131.

[33] Stephen Barr, "Probe Finds IRS Workers Were 'Browsing' in Files," *The Washington Post,* 3 August 1993, A1.

[34] Charles Piller, "Special Report: Workplace and Consumer Privacy Under Siege," *MacWorld* (July 1993): 1-14.