normally work with program and functional mangers/application owners, the computer security staff, and others to obtain additional contingency planning support, as needed.

Quality Assurance. 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 of the program, for example, by improving the integrity of computer-based information, the availability of services, and the confidentiality of customer information, as appropriate.

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 it lacks the technical expertise. Nevertheless, this office should be knowledgeable about computer security standards and should bring them to the attention of those requesting such technology.

Training Office. An organization has to 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. The personnel and security offices normally work closely on issues involving background investigations. The personnel office may also be responsible for providing security-related exit procedures when employees leave an organization.

Risk Management/Planning Staff. Some organizations have a full-time staff devoted to studying all types of risks to which the organization may be exposed. This function should include computer security-related risks, although this office normally focuses on "macro" issues. Specific risk analyses for specific computer systems is normally not performed by this office.

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.

3.6 Users

Users also have responsibilities for computer security. Two kinds of users, and their associated responsibilities, are described below.

Users of Information. Individuals who use information provided by the computer can be considered the "consumers" of the applications. Sometimes they directly interact with the system (e.g., to generate a report on screen) – in which case they are also users of the system (as discussed below). Other times, they may only read computer-prepared reports or only be briefed on such material. Some users of information may be very far removed from the computer system. Users of information are responsible for letting the functional mangers/application owners (or their representatives) know what their needs are for the protection of information, especially for its integrity and availability.

Users of Systems. Individuals who directly use computer systems (typically via a keyboard) are responsible for following security procedures, for reporting security problems, and for attending required computer security and functional training.

References

Wood, Charles Cresson. "How to Achieve a Clear Definition of Responsibilities for Information Security." DATAPRO Information Security Service, IS115-200-101, 7 pp. April 1993.

Chapter 4

COMMON THREATS: A BRIEF OVERVIEW

Computer systems are vulnerable to many threats that can inflict various types of damage resulting in significant losses. This damage can range from errors harming database integrity to fires destroying entire computer centers. Losses can stem, for example, from the actions of supposedly trusted employees defrauding a system, from outside hackers, or from careless data entry clerks. Precision in estimating computer security-related losses is not possible because many losses are never discovered, and others are "swept under the carpet" to avoid unfavorable publicity. The effects of various threats varies considerably: some affect the confidentiality or integrity of data while others affect the availability of a system.

This chapter presents a broad view of the risky environment in which systems operate today. The threats and associated losses presented in this chapter 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.[19] 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. Thus, threats against particular systems could be quite different from those discussed here.[20]

To control the risks of operating an information system, managers and users need to know the vulnerabilities of the system and the threats that may exploit them. Knowledge of the threat[21] environment allows the system manager to implement the most cost-effective security measures. In some cases, managers may find it more cost-effective to simply tolerate the expected losses. Such decisions should be based on the results of a risk analysis. (See Chapter 7.)

---

[19] As is true for this publication as a whole, this chapter does not address threats to national security systems, which fall outside of NIST's purview. The term "national security systems" is defined in National Security Directive 42 (7/5/90) as being "those telecommunications and information systems operated by the U.S. Government, its contractors, or agents, that contain classified information or, as set forth in 10 U.S.C. 2315, that involves intelligence activities, involves cryptologic activities related to national security, involves command and control of military forces, involves equipment that is an integral part of a weapon or weapon system, or involves equipment that is critical to the direct fulfillment of military or intelligence missions."

[20] A discussion of how threats, vulnerabilities, safeguard selection and risk mitigation are related is contained in Chapter 7, Risk Management.

[21] Note that one protects against threats that can exploit a vulnerability. If a vulnerability exists but no threat exists to take advantage of it, little or nothing is gained by protecting against the vulnerability. See Chapter 7, Risk Management.

4.1 Errors and Omissions

Errors and omissions are an important threat to data and system integrity. These errors are caused not only by data entry clerks processing hundreds of transactions per day, but also 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. A sound awareness and training program can help an organization reduce the number and severity of errors and omissions.

Users, data entry clerks, system operators, and programmers frequently make errors that contribute directly or indirectly to security problems. In some cases, the error 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 systems 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.[22] This figure was relatively consistent between both private and public sector organizations.

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.[23]

Since the study's publication, 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. While there have been great

---

[22] Computer System Security and Privacy Advisory Board, *1991 Annual Report* (Gaithersburg, MD), March 1992, p. 18. The categories into which the problems were placed and the percentages of economic loss attributed to each were: 65%, errors and omissions; 13%, dishonest employees; 6%, disgruntled employees; 8%, loss of supporting infrastructure, including power, communications, water, sewer, transportation, fire, flood, civil unrest, and strikes; 5%, water, not related to fires and floods; less than 3%, outsiders, including viruses, espionage, dissidents, and malcontents of various kinds, and former employees who have been away for more than six weeks.

[23] 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, p. 2.

improvements in program quality, as reflected in decreasing errors per 1000 lines of code, the concurrent growth in program size often seriously diminishes the beneficial effects of these program quality enhancements.

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.[24]

4.2 Fraud and Theft

Computer systems can be exploited for both fraud and theft 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, assuming that small discrepancies may not be investigated. Financial systems are not the only ones at risk. Systems that control access to any resource are targets (e.g., time and attendance systems, inventory systems, school grading systems, and long-distance telephone systems).

Computer fraud and theft can be committed by insiders or outsiders. Insiders (i.e., authorized users of a system) are responsible for the majority of fraud. 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.[25] The U.S. Department of Justice's Computer Crime Unit contends that "insiders constitute the greatest threat to computer systems."[26] Since insiders have both access to and familiarity with the victim computer system (including what resources it controls and its flaws), authorized system users are in a better position to commit crimes. Insiders can be both general users (such as clerks) or technical staff members. An organization's former employees, with their knowledge of an organization's operations, may also pose a threat, particularly if their access is not terminated promptly.

In addition to the use of technology to commit fraud and theft, computer hardware and software may be vulnerable to theft. For example, one study conducted by Safeware Insurance found that $882 million worth of personal computers was lost due to theft in 1992.[27]

---

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

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

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

[27] "Theft, Power Surges Cause Most PC Losses," *Infosecurity News*, September/October, 1993, 13.

4.3 Employee Sabotage

Common examples of computer-related employee sabotage include:

- destroying hardware or facilities,
- planting logic bombs that destroy programs or data,
- entering data incorrectly,
- "crashing" systems,
- deleting data,
- holding data hostage, and
- changing data.

Employees are most familiar with their employer's computers and applications, including knowing what actions might cause the most damage, mischief, or sabotage. 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 are not deleted in a timely manner).[28] The number of incidents of employee sabotage is believed to be much smaller than the instances of theft, but the cost of such incidents can be quite high.

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.[29]

4.4 Loss of Physical and Infrastructure Support

The loss of supporting infrastructure includes power failures (outages, spikes, and brownouts), loss of communications, water outages and leaks, sewer problems, lack of transportation services, fire, flood, civil unrest, and strikes. These losses include such dramatic events as the explosion at the World Trade Center and the Chicago tunnel flood, as well as more common events, such as broken water pipes. Many of these issues are covered in Chapter 15. 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.

4.5 Malicious Hackers

The term *malicious hackers*, sometimes called *crackers*, refers to those who break into computers

[28] Charney.

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

without authorization. They can include both outsiders and insiders. Much of the rise of hacker activity is often attributed to increases in connectivity in both government and industry. One 1992 study of a particular Internet site (i.e., one computer system) found that hackers attempted to break in at least once every other day.[30]

The hacker threat should be considered in terms of past and potential future damage. Although current losses due to hacker attacks are significantly smaller than losses due to insider theft and sabotage, the hacker problem is widespread and serious. One example of malicious hacker activity is that directed against the public telephone system.

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.[31, 32]

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 measures are ineffective against outsiders who are not subject to the rules and regulations of the employer.

- Second, organizations do not know the purposes of a hacker – some hackers 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, particularly because their identity is 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 may 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

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

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

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

piece of jewelry, the entire neighborhood may feel victimized and vulnerable.[33]

4.6 Industrial Espionage

Industrial espionage is the act of gathering proprietary data from private companies or the government[34] 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. Since information is processed and stored on computer systems, computer security can help protect against such threats; it can do little, however, to reduce the threat of authorized employees selling that information.

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 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.[35] 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.[36]

Within the area of economic espionage, the Central Intelligence Agency 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.[37] 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.[38]

---

[33] Charney.

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

[35] The figures of 30 and 58 percent are not mutually exclusive.

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

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

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

4.7 Malicious Code

Malicious code refers to viruses, worms, Trojan horses, logic bombs, and other "uninvited" software. Sometimes mistakenly associated only with personal computers, malicious code can attack other platforms.

A 1993 study of viruses found that while the number of known viruses is increasing exponentially, the number of virus incidents is not.[39] 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.[40, 41]

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 that 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 that also includes unexpected (and undesirable) functions. Consider as an example an editing program for a multiuser 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 that 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 use network services to propagate to other host systems.
Source: NIST Special Publication 800-5.

4.8 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

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

[40] Ibid.

[41] Estimates of virus occurrences may not consider the strength of an organization's antivirus program.

systems to further their intelligence missions. Some unclassified information that may be of interest includes travel plans of senior officials, civil defense and emergency preparedness, manufacturing technologies, satellite data, personnel and payroll data, and law enforcement, investigative, and security files. Guidance should be sought from the cognizant security office regarding such threats.

4.9 Threats to Personal Privacy

The accumulation of vast amounts of electronic information about individuals by governments, credit bureaus, and private companies, combined with the ability of computers to monitor, process, and aggregate large amounts of information about individuals have created a threat to individual privacy. The possibility that all of this information and technology may be able to be linked together has arisen as a specter of the modern information age. This is often referred to as "Big Brother." To guard against such intrusion, Congress has enacted legislation, over the years, 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.

The threat to personal privacy arises from many sources. In several cases federal and state employees have sold personal information 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.[42] During the investigation, auditors learned that SSA employees had unrestricted access to over 130 million employment records. Another investigation found that 5 percent of the employees in one region of the IRS had browsed through tax records of friends, relatives, and celebrities.[43] 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

---

[42] 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.

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

concerned about personal privacy. By 1990, that number had jumped to 79 percent.[44]

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.

References

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 Congress, 1st session, August 3, 1989.

National Research Council. *Computers at Risk: Safe Computing in the Information Age*. Washington, DC: National Academy Press, 1991.

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

Neumann, Peter G. *Computer-Related Risks*. Reading, MA: Addison-Wesley, 1994.

Schwartau, W. *Information Warfare*. New York, NY: Thunders Mouth Press, 1994 (Rev. 1995).

Sprouse, Martin, ed. *Sabotage in the American Workplace: Anecdotes of Dissatisfaction, Mischief, and Revenge*. San Francisco, CA: Pressure Drop Press, 1992.

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

II. MANAGEMENT CONTROLS

Chapter 5

COMPUTER SECURITY POLICY

In discussions of computer security, the term *policy* has more than one meaning.[45] *Policy* is senior management's directives to create a computer security program, establish its goals, and assign responsibilities. The term *policy* is also used to refer to the specific security rules for particular systems.[46] Additionally, *policy* may refer to entirely different matters, such as the specific managerial decisions setting an organization's e-mail privacy policy or fax security policy.

Policy means different things to different people. The term "policy" is used in this chapter in a broad manner to refer to important computer security-related decisions.

In this chapter the term *computer security policy* is defined as the "documentation of computer security decisions" – which covers all the types of policy described above.[47] In making these decisions, managers face hard choices involving resource allocation, competing objectives, and organizational strategy related to protecting both technical and information resources as well as guiding employee behavior. Managers at all levels make choices that can result in policy, with the scope of the policy's applicability varying according to the scope of the manager's authority. In this chapter we use the term *policy* in a broad manner to encompass all of the types of policy described above – regardless of the level of manager who sets the particular policy.

Managerial decisions on computer security issues vary greatly. To differentiate among various kinds of policy, this chapter categorizes them into three basic types:

- *Program policy* is used to create an organization's computer security program.
- *Issue-specific policies* address specific issues of concern to the organization.

---

[45] There are variations in the use of the term *policy*, as noted in a 1994 Office of Technology Assessment report, *Information Security and Privacy in Network Environments*: "*Security Policy* refers here to the statements made by organizations, corporations, and agencies to establish overall policy on information access and safeguards. Another meaning comes from the Defense community and refers to the rules relating clearances of users to classification of information. In another usage, *security policies* are used to refine and implement the broader, organizational security policy...."

[46] These are the kind of policies that computer security experts refer to as being *enforced* by the system's technical controls as well as its management and operational controls.

[47] In general, policy is set by a manager. However, in some cases, it may be set by a group (e.g., an intraorganizational policy board).

- *System-specific policies* focus on decisions taken by management to protect a particular system.[48]

Procedures, standards, and guidelines are used to describe how these policies will be implemented within an organization. (See following box.)

Tools to Implement Policy:
Standards, Guidelines, and Procedures

Because policy is written at a broad level, organizations also develop standards, guidelines, and procedures that offer users, managers, and others a clearer approach to implementing policy and meeting organizational goals. Standards and guidelines specify technologies and methodologies to be used to secure systems. Procedures are yet more detailed steps to be followed to accomplish particular security-related tasks. Standards, guidelines, and procedures may be promulgated throughout an organization via handbooks, regulations, or manuals.

Organizational standards (not to be confused with American National Standards, FIPS, Federal Standards, or other national or international standards) specify uniform use of specific technologies, parameters, or procedures when such uniform use will benefit an organization. Standardization of organizationwide identification badges is a typical example, providing ease of employee mobility and automation of entry/exit systems. Standards are normally compulsory within an organization.

Guidelines assist users, systems personnel, and others in effectively securing their systems. The nature of guidelines, however, immediately recognizes that systems vary considerably, and imposition of standards is not always achievable, appropriate, or cost-effective. For example, an organizational guideline may be used to help develop system-specific standard procedures. Guidelines are often used to help ensure that specific security measures are not overlooked, although they can be implemented, and correctly so, in more than one way.

Procedures normally assist in complying with applicable security policies, standards, and guidelines. They are detailed steps to be followed by users, system operations personnel, or others to accomplish a particular task (e.g., preparing new user accounts and assigning the appropriate privileges).

Some organizations issue overall computer security manuals, regulations, handbooks, or similar documents. These may mix policy, guidelines, standards, and procedures, since they are closely linked. While manuals and regulations can serve as important tools, it is often useful if they clearly distinguish between policy and its implementation. This can help in promoting flexibility and cost-effectiveness by offering alternative implementation approaches to achieving policy goals.

[48] A *system* refers to the entire collection of processes, both those performed manually and those using a computer (e.g., manual data collection and subsequent computer manipulation), which performs a function. This includes both application systems and support systems, such as a network.

Familiarity with various types and components of policy will aid managers in addressing computer security issues important to the organization. Effective policies ultimately result in the development and implementation of a better computer security program and better protectio n of systems and information.

These types of policy are described to aid the reader's understanding.[49] It is not important that one categorizes specific organizational policies into these three categories; it is more important to focus on the functions of each.

5.1 Program Policy

A management official, normally the head of the organization or the senior administration official, issues program policy to establish (or restructure) the organization's computer security program and its basic structure. This high-level policy defines the purpose of the program and its scope within the organization; assigns responsibilities (to the computer security organization) for direct program implementation, as well as other responsibilities to related offices (such as the Information Resources Management [IRM] organization); and addresses compliance issues.

Program policy sets organizational strategic directions for security and assigns resources for its implementation.

5.1.1 Basic Components of Program Policy

Components of program policy should address:

Purpose. Program policy normally includes a statement describing why the program is being established. This may include defining the *goals* of the program. Security-related needs, such as integrity, availability, and confidentiality, can form the basis of organizational goals established in policy. For instance, in an organization responsible for maintaining large mission-critical databases, reduction in errors, data loss, data corruption, and recovery might be specifically stressed. In an organization responsible for maintaining confidential personal data, however, goals might emphasize stronger protection against unauthorized disclosure.

Scope. Program policy should be clear as to which resources -- including facilities, hardware, and software, information, and personnel -- the computer security program covers. In many cases, the program will encompass all systems and organizational personnel, but this is not always true. In some instances, it may be appropriate for an organization's computer security program to be more limited in scope.

[49] No standard terms exist for various types of policies. These terms are used to aid the reader's understanding of this topic; no implication of their widespread usage is intended.

Responsibilities. Once the computer security program is established, its management is normally assigned to either a newly created or existing office.[50]

Program policy establishes the security program and assigns program management and supporting responsibilities.

The responsibilities of officials and offices throughout the organization also need to be addressed, including line managers, applications owners, users, and the data processing or IRM organizations. This section of the policy statement, for example, would distinguish between the responsibilities of computer services providers and those of the managers of applications using the provided services. The policy could also establish operational security offices for major systems, particularly those at high risk or most critical to organizational operations. It also can serve as the basis for establishing employee accountability.

At the program level, responsibilities should be specifically assigned to those organizational elements and officials responsible for the implementation and continuity of the computer security policy.[51]

Compliance. Program policy typically will address two compliance issues:

1. General compliance to ensure meeting the requirements to establish a program and the responsibilities assigned therein to various organizational components. Often an oversight office (e.g., the Inspector General) is assigned responsibility for monitoring compliance, including how well the organization is implementing management's priorities for the program.

2. The use of specified penalties and disciplinary actions. Since the security policy is a high-level document, specific penalties for various infractions are normally not detailed here; instead, the policy may authorize the creation of compliance structures that include violations and specific disciplinary action(s).[52]

---

[50] The program management structure should be organized to best address the goals of the program and respond to the particular operating and risk environment of the organization. Important issues for the structure of the computer security program include management and coordination of security-related resources, interaction with diverse communities, and the ability to relay issues of concern, trade-offs, and recommended actions to upper management. (See Chapter 6, Computer Security Program Management.)

[51] In assigning responsibilities, it is necessary to be specific; such assignments as "computer security is everyone's responsibility," in reality, mean no one has specific responsibility.

[52] The need to obtain guidance from appropriate legal counsel is critical when addressing issues involving penalties and disciplinary action for individuals. The policy does not need to restate penalties already provided

Those developing compliance policy should remember that violations of policy can be unintentional on the part of employees. For example, nonconformance can often be due to a lack of knowledge or training.

5.2 Issue-Specific Policy

Whereas program policy is intended to address the broad organizationwide computer security program, issue-specific policies are developed to focus on areas of current relevance and concern (and sometimes controversy) to an organization. Management may find it appropriate, for example, to issue a policy on how the organization will approach contingency planning (centralized vs. decentralized) or the use of a particular methodology for managing risk to systems. A policy could also be issued, for example, on the appropriate use of a cutting-edge technology (whose security vulnerabilities are still largely unknown) within the organization. Issue-specific policies may also be appropriate when new issues arise, such as when implementing a recently passed law requiring additional protection of particular information. Program policy is usually broad enough that it does not require much modification over time, whereas issue-specific policies are likely to require more frequent revision as changes in technology and related factors take place.

In general, for issue-specific and system-specific policy, the issuer is a senior official; the more global, controversial, or resource-intensive, the more senior the issuer.

5.2.1 Example Topics for Issue-Specific Policy[53]

Both new technologies and the appearance of new threats often require the creation of issue-specific policies.

There are many areas for which issue-specific policy may be appropriate. Two examples are explained below.

Internet Access. Many organizations are looking at the Internet as a means for expanding their research opportunities and communications. Unquestionably, connecting to the Internet yields many benefits – and some disadvantages. Some issues an Internet access policy may address include who will have access, which types of systems may be connected to the network, what types of information may be transmitted via the network, requirements for user authentication for Internet-connected systems, and the use of firewalls and secure gateways.

---

for by law, although they can be listed if the policy will also be used as an awareness or training document.

[53] Examples presented in this section are not all-inclusive nor meant to imply that policies in each of these areas are required by all organizations.

E-Mail Privacy. Users of computer e-mail systems have come to rely upon that service for informal communication with colleagues and others. However, since the system is typically owned by the employing organization, from time-to-time, management may wish to monitor the employee's e-mail for various reasons (e.g., to be sure that it is used for business purposes only or if they are suspected of distributing viruses, sending offensive e-mail, or disclosing organizational secrets.) On the other hand, users may have an expectation of privacy, similar to that accorded U.S. mail. Policy in this area addresses what level of privacy will be accorded e-mail and the circumstances under which it may or may not be read.

Other potential candidates for issue-specific policies include: approach to risk management and contingency planning, protection of confidential/proprietary information, unauthorized software, acquisition of software, doing computer work at home, bringing in disks from outside the workplace, access to other employees' files, encryption of files and e-mail, rights of privacy, responsibility for correctness of data, suspected malicious code, and physical emergencies.

5.2.2 Basic Components of Issue-Specific Policy

As suggested for program policy, a useful structure for issue-specific policy is to break the policy into its basic components.

Issue Statement. To formulate a policy on an issue, managers first must define the issue with any relevant terms, distinctions, and conditions included. It is also often useful to specify the goal or justification for the policy – which can be helpful in gaining compliance with the policy. For example, an organization might want to develop an issue-specific policy on the use of "unofficial software," which might be defined to mean any software not approved, purchased, screened, managed, and owned by the organization. Additionally, the applicable distinctions and conditions might then need to be included, for instance, for software privately owned by employees but approved for use at work, and for software owned and used by other businesses under contract to the organization.

Statement of the Organization's Position. Once the issue is stated and related terms and conditions are discussed, this section is used to clearly state the organization's position (i.e., management's decision) on the issue. To continue the previous example, this would mean stating whether use of unofficial software as defined is prohibited in all or some cases, whether there are further guidelines for approval and use, or whether case-by-case exceptions will be granted, by whom, and on what basis.

Applicability. Issue-specific policies also need to include statements of applicability. This means clarifying where, how, when, to whom, and to what a particular policy applies. For example, it could be that the hypothetical policy on unofficial software is intended to apply only to the organization's own on-site resources and employees and not to contractors with offices at other

locations. Additionally, the policy's applicability to employees travelling among different sites and/or working at home who need to transport and use disks at multiple sites might need to be clarified.

Roles and Responsibilities. The assignment of roles and responsibilities is also usually included in issue-specific policies. For example, if the policy permits unofficial software privately owned by employees to be used at work with the appropriate approvals, then the approval authority granting such permission would need to be stated. (Policy would stipulate, who, by position, has such authority.) Likewise, it would need to be clarified who would be responsible for ensuring that only approved software is used on organizational computer resources and, perhaps, for monitoring users in regard to unofficial software.

Compliance. For some types of policy, it may be appropriate to describe, in some detail, the infractions that are unacceptable, and the consequences of such behavior. Penalties may be explicitly stated and should be consistent with organizational personnel policies and practices. When used, they should be coordinated with appropriate officials and offices and, perhaps, employee bargaining units. It may also be desirable to task a specific office within the organization to monitor compliance.

Points of Contact and Supplementary Information. For any issue-specific policy, the appropriate individuals in the organization to contact for further information, guidance, and compliance should be indicated. Since positions tend to change less often than the people occupying them, specific positions may be preferable as the point of contact. For example, for some issues the point of contact might be a line manager; for other issues it might be a facility manager, technical support person, system administrator, or security program representative. Using the above example once more, employees would need to know whether the point of contact for questions and procedural information would be their immediate superior, a system

Some Helpful Hints on Policy

To be effective, policy requires visibility. Visibility aids implementation of policy by helping to ensure policy is fully communicated throughout the organization. Management presentations, videos, panel discussions, guest speakers, question/answer forums, and newsletters increase visibility. The organization's computer security training and awareness program can effectively notify users of new policies. It also can be used to familiarize new employees with the organization's policies.

Computer security policies should be introduced in a manner that ensures that management's unqualified support is clear, especially in environments where employees feel inundated with policies, directives, guidelines, and procedures. The organization's policy is the vehicle for emphasizing management's commitment to computer security and making clear their expectations for employee performance, behavior, and accountability.

To be effective, policy should be consistent with other existing directives, laws, organizational culture, guidelines, procedures, and the organization's overall mission. It should also be integrated into and consistent with other organizational policies (e.g., personnel policies). One way to help ensure this is to coordinate policies during development with other organizational offices.

administrator, or a computer security official.

Guidelines and procedures often accompany policy. The issue-specific policy on unofficial software, for example, might include procedural guidelines for checking disks brought to work that had been used by employees at other locations.

5.3 System-Specific Policy

Program policy and issue-specific policy both address policy from a broad level, usually encompassing the entire organization. However, they do not provide sufficient information or direction, for example, to be used in establishing an access control list or in training users on what actions are permitted. System-specific policy fills this need. It is much more focused, since it addresses only one system.

Many security policy decisions may apply only at the system level and may vary from system to system within the same organization. While these decisions may appear to be too detailed to be policy, they can be extremely important, with significant impacts on system usage and security. These types of decisions can be made by a *management official*, not by a technical system administrator.[54] (The impacts of these decisions, however, are often analyzed by technical system administrators.)

System-specific security policy includes two components: security objectives and operational security rules. It is often accompanied by implementing procedures and guidelines.

To develop a cohesive and comprehensive set of security policies, officials may use a management process that derives security rules from security goals. It is helpful to consider a two-level model for system security policy: security objectives and operational security rules, which together comprise the system-specific policy. Closely linked and often difficult to distinguish, however, is the implementation of the policy in technology.

5.3.1 Security Objectives

Sample Security Objective

Only individuals in the accounting and personnel departments are authorized to provide or modify information used in payroll processing.

The first step in the management process is to define security objectives for the specific system. Although, this process may start with an analysis of the need for integrity,

[54] It is important to remember that policy is not created in a vacuum. For example, it is critical to understand the system mission and how the system is intended to be used. Also, users may play an important role in setting policy.

availability, and confidentiality, it should not stop there. A security *objective* needs to more specific; it should be concrete and well defined. It also should be stated so that it is clear that the objective is achievable. This process will also draw upon other applicable organization policies.

Security objectives consist of a series of statements that describe meaningful actions about explicit resources. These objectives should be based on system functional or mission requirements, but should state the security actions that support the requirements.

Development of system-specific policy will require management to make trade-offs, since it is unlikely that all desired security objectives will be able to be fully met. Management will face cost, operational, technical, and other constraints.

5.3.2 Operational Security Rules

After management determines the security objectives, the rules for operating a system can be laid out, for example, to define authorized and unauthorized modification. Who (by job category, organization placement, or name) can do what (e.g., modify, delete) to which specific classes and records of data, and under what conditions.

Sample Operational Security Rule

Personnel clerks may update fields for weekly attendance, charges to annual leave, employee addresses, and telephone numbers. Personnel specialists may update salary information. No employees may update their own records.

The degree of specificity needed for operational security rules varies greatly. The more detailed the rules are, *up to a point*, the easier it is to know when one has been violated. It is also, *up to a point*, easier to automate policy enforcement. However, overly detailed rules may make the job of instructing a computer to implement them difficult or computationally complex.

In addition to deciding the level of detail, management should decide the degree of formality in documenting the system-specific policy. Once again, the more formal the documentation, the easier it is to enforce and to follow policy. On the other hand, policy at the system level that is too detailed and formal can also be an administrative burden. In general, good practice suggests a reasonably detailed formal statement of the access privileges for a system. Documenting access controls policy will make it substantially easier to follow and to enforce. (See Chapters 10 and 17, Personnel/User Issues and Logical Access Control.) Another area that normally requires a detailed and formal statement is the assignment of security responsibilities. Other areas that should be addressed are the rules for system usage and the consequences of noncompliance.

Policy decisions in other areas of computer security, such as those described in this handbook, are often documented in the risk analysis, accreditation statements, or procedural manuals. However,

any controversial, atypical, or uncommon policies will also need formal statements. Atypical policies would include any areas where the system policy is different from organizational policy or from normal practice within the organization, either more or less stringent. The documentation for a typical policy contains a statement explaining the reason for deviation from the organization's standard policy.

5.3.3 System-Specific Policy Implementation

Technology plays an important – but not sole – role in enforcing system-specific policies. When technology is used to enforce policy, it is important not to neglect nontechnology- based methods. For example, technical system-based controls could be used to limit the printing of confidential reports to a particular printer. However, corresponding physical security measures would also have to be in place to limit access to the printer output or the desired security objective would not be achieved.

Technical methods frequently used to implement system-security policy are likely to include the use of *logical access controls*. However, there are other automated means of enforcing or supporting security policy that typically supplement logical access controls. For example, technology can be used to block telephone users from calling certain numbers. Intrusion-detection software can alert system administrators to suspicious activity or can take action to stop the activity. Personal computers can be configured to prevent booting from a floppy disk.

Technology-based enforcement of system-security policy has both advantages and disadvantages. A computer system, properly designed, programmed, installed, configured, and maintained,[55] consistently enforces policy within the computer system, although no computer can force users to follow all procedures. Management controls also play an important role – and should not be neglected. In addition, deviations from the policy may sometimes be necessary and appropriate; such deviations may be difficult to implement easily with some technical controls. This situation occurs frequently if implementation of the security policy is too rigid (which can occur when the system analysts fail to anticipate contingencies and prepare for them).

5.4 Interdependencies

Policy is related to many of the topics covered in this handbook:

Program Management. Policy is used to establish an organization's computer security program, and is therefore closely tied to program management and administration. Both program and system-specific policy may be established in any of the areas covered in this handbook. For

[55] Doing all of these things properly is, unfortunately, the exception rather than the rule. Confidence in the system's ability to enforce system-specific policy is closely tied to assurance. (See Chapter 9, Assurance.)

example, an organization may wish to have a consistent approach to incident handling for all its systems – and would issue appropriate program policy to do so. On the other hand, it may decide that its applications are sufficiently independent of each other that application managers should deal with incidents on an individual basis.

Access Controls. System-specific policy is often implemented through the use of access controls. For example, it may be a policy decision that only two individuals in an organization are authorized to run a check-printing program. Access controls are used by the system to implement (or enforce) this policy.

Links to Broader Organizational Policies. This chapter has focused on the types and components of computer security policy. However, it is important to realize that *computer* security policies are often *extensions* of an organization's *information* security policies for handling information in other forms (e.g., paper documents). For example, an organization's e-mail policy would probably be tied to its broader policy on privacy. Computer security policies may also be extensions of other policies, such as those about appropriate use of equipment and facilities.

5.5 Cost Considerations

A number of potential costs are associated with developing and implementing computer security policies. Overall, the major cost of policy is the cost of implementing the policy and its impacts upon the organization. For example, establishing a computer security program, accomplished through policy, does not come at negligible cost.

Other costs may be those incurred through the policy development process. Numerous administrative and management activities may be required for drafting, reviewing, coordinating, clearing, disseminating, and publicizing policies. In many organizations, successful policy implementation may require additional staffing and training – and can take time. In general, the costs to an organization for computer security policy development and implementation will depend upon how extensive the change needed to achieve a level of risk acceptable to management.

References

Howe, D. "Information System Security Engineering: Cornerstone to the Future." *Proceedings of the 15th National Computer Security Conference*. Baltimore, MD, Vol. 1, October 15, 1992. pp. 244-251.

Fites, P., and M. Kratz. "Policy Development." *Information Systems Security: A Practitioner's Reference*. New York, NY: Van Nostrand Reinhold, 1993. pp. 411-427.

Lobel, J. "Establishing a System Security Policy." *Foiling the System Breakers*. New York, NY: McGraw-Hill, 1986. pp. 57-95.

Menkus, B. "Concerns in Computer Security." *Computers and Security*. 11(3), 1992. pp. 211-215.

Office of Technology Assessment. "Federal Policy Issues and Options." *Defending Secrets, Sharing Data: New Locks for Electronic Information*. Washington, DC: U.S Congress, Office of Technology Assessment, 1987. pp. 151-160.

Office of Technology Assessment. "Major Trends in Policy Development." *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information*. Washington, DC: U.S. Congress, Office of Technology Assessment, 1987. p. 131-148.

O'Neill, M., and F. Henninge, Jr. "Understanding ADP System and Network Security Considerations and Risk Analysis." *ISSA Access*. 5(4), 1992. pp. 14-17.

Peltier, Thomas. "Designing Information Security Policies That Get Results." *Infosecurity News*. 4(2), 1993. pp. 30-31.

President's Council on Management Improvement and the President's Council on Integrity and Efficiency. *Model Framework for Management Control Over Automated Information System*. Washington, DC: President's Council on Management Improvement, January 1988.

Smith, J. "Privacy Policies and Practices: Inside the Organizational Maze." *Communications of the ACM*. 36(12), 1993. pp. 104-120.

Sterne, D. F. "On the Buzzword `Computer Security Policy.'" In *Proceedings of the 1991 IEEE Symposium on Security and Privacy*, Oakland, CA: May 1991. pp. 219-230.

Wood, Charles Cresson. "Designing Corporate Information Security Policies." *DATAPRO Reports on Information Security*, April 1992.

Chapter 6

COMPUTER SECURITY PROGRAM MANAGEMENT

Computers and the information they process are critical to many organizations' ability to perform their mission and business functions.[56] It therefore makes sense that executives view computer security as a management issue and seek to protect their organization's computer resources as they would any other valuable asset. To do this effectively requires developing of a comprehensive management approach.

This chapter presents an organizationwide approach to computer security and discusses its important management function.[57] Because organizations differ vastly in size, complexity, management styles, and culture, it is not possible to describe one ideal computer security program. However, this chapter does describe some of the features and issues common to many federal organizations.

> OMB Circular A-130, "Management of Federal Information Resources," requires that federal agencies establish computer security programs.

6.1 Structure of a Computer Security Program

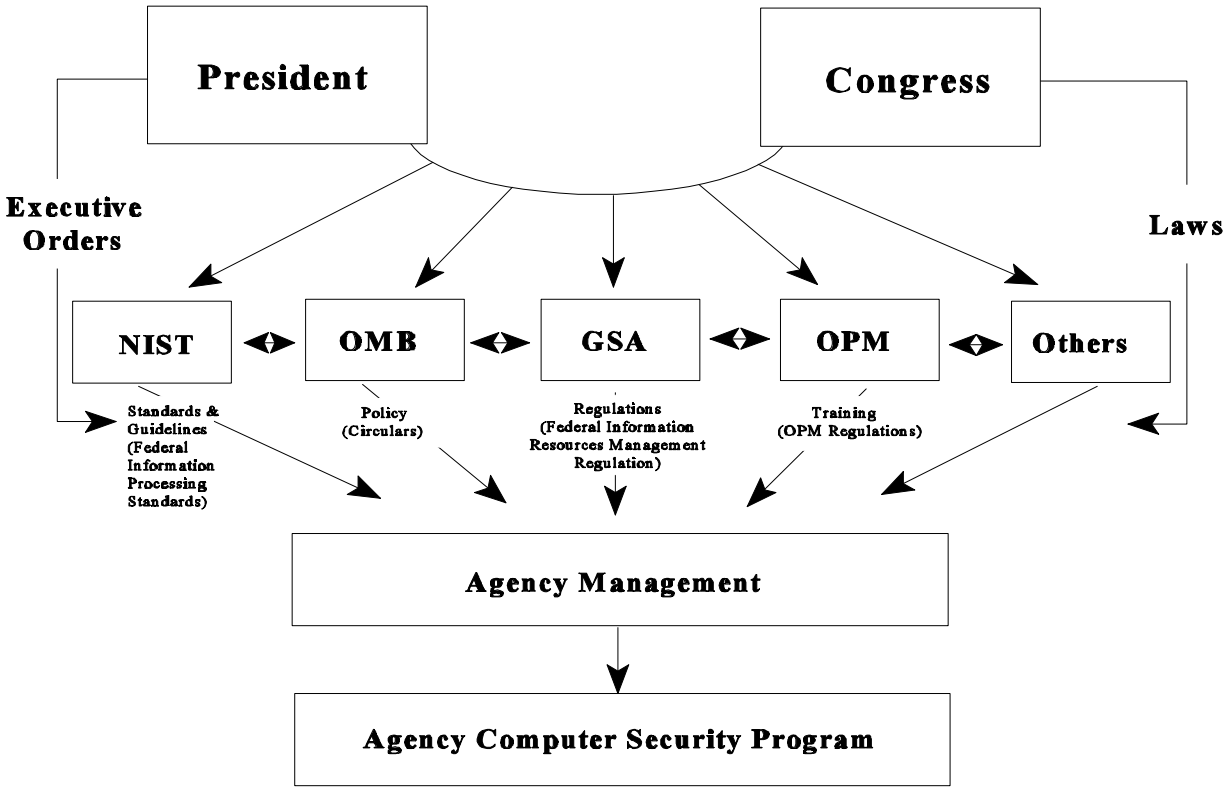
Many computer security programs that are distributed throughout the organization have different elements performing various functions. While this approach has benefits, the distribution of the computer security function in many organizations is haphazard, usually based upon history (i.e., who was available in the organization to do what when the need arose). Ideally, the distribution of computer security functions should result from a planned and integrated management philosophy.

Managing computer security at multiple levels brings many benefits. Each level contributes to the overall computer security program with different types of expertise, authority, and resources. In general, higher-level officials (such as those at the headquarters or unit levels in the agency described above) better understand the organization as a whole and have more authority. On the other hand, lower-level officials (at the computer facility and applications levels) are more familiar with the specific requirements, both technical and procedural, and problems of the systems and

[56] This chapter is primarily directed at federal agencies, which are generally very large and complex organizations. This chapter discusses programs which are suited to managing security in such environments. They may be wholly inappropriate for smaller organizations or private sector firms.

[57] This chapter addresses the management of security programs, not the various activities such as risk analysis or contingency planning that make up an effective security program.

Sources of (Some) Requirements for Federal Unclassified Computer Security Programs



A federal agency computer security program is created and operates in an environment rich in guidance and direction from other organizations. Figure 6.1 illustrates some of the external sources of requirements and guidance directed toward agency management with regard to computer security. While a full discussion of each is outside the scope of this chapter, it is important to realize that a program does not operate in a vacuum; federal organizations are constrained -- by both statute and regulation -- in a number of ways.

Figure 6.1

the users. The levels of computer security program management should be complementary; each can help the other be more effective.

Since many organizations have at least two levels of computer security management, this chapter divides computer security program management into two levels: the *central* level and the *system* level. (Each organization, though, may have its own unique structure.) The central computer

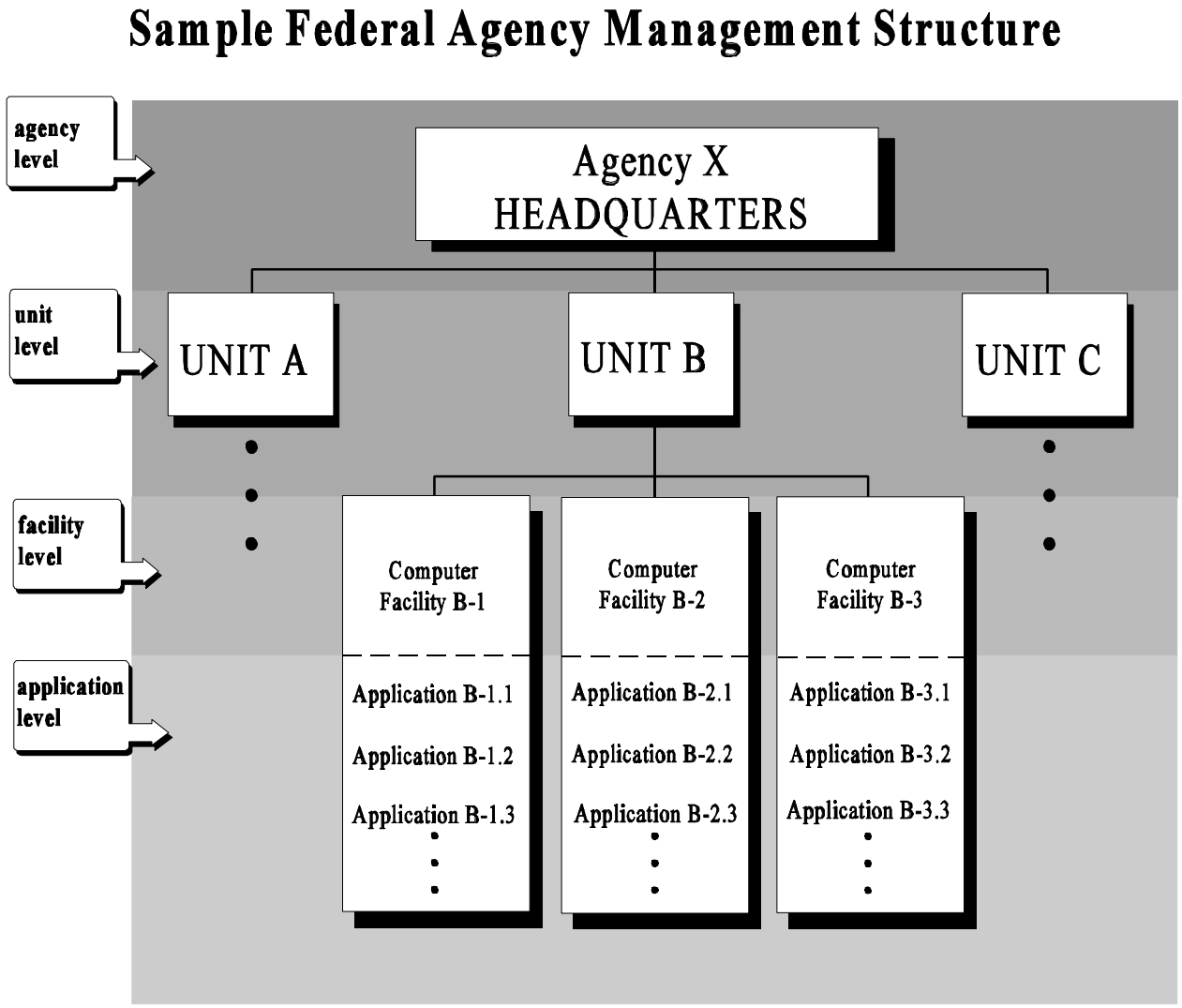


Figure 6.2 shows a management structure based on that of an actual federal agency. The agency consists of three major units, each with several large computer facilities running multiple applications. This type of organization needs to manage computer security at the *agency* level, the *unit* level, the *computer facility* level, and the *application* level.

Figure 6.2

security program can be used to address the overall management of computer security within an organization or a major component of an organization. The system-level computer security program addresses the management of computer security for a particular system.

6.2 Central Computer Security Programs

The purpose of a central computer security program is to address the overall management of

computer security within an organization. In the federal government, the organization could consist of a department, agency, or other major operating unit.

As with the management of all resources, central computer security management can be performed in many practical and cost-effective ways. The importance of sound management cannot be overemphasized. There is also a downside to centrally managed computer security programs. Specifically, they present greater risk that errors in judgement will be more widely propagated throughout the organization. As they strive to meet their objectives, managers need to consider the full impact of available options when establishing their computer security programs.

6.2.1 Benefits of Central Computer Security Programs

A central security program should provide two quite distinct types of benefits:

- Increased efficiency and economy of security throughout the organization, and
- the ability to provide centralized enforcement and oversight.

Both of these benefits are in keeping with the purpose of the Paperwork Reduction Act, as implemented in OMB Circular A-130.

> The Paperwork Reduction Act establishes a broad mandate for agencies to perform their information management activities in an efficient, effective, and economical manner... . Agencies shall assure an adequate level of security for all agency automated information systems, whether maintained in-house or commercially.[58]

6.2.2 Efficient, Economic Coordination of Information

A central computer security program helps to coordinate and manage effective use of security-related resources throughout the organization. The most important of these resources are normally *information* and *financial resources*.

Sound and timely information is necessary for managers to accomplish their tasks effectively. However, most organizations have trouble collecting information from myriad sources and effectively processing and distributing it within the organization. This section discusses some of the sources and efficient uses of *computer security* information.

Within the federal government, many organizations such as the Office of Management and

[58] OMB Circular A-130, Section 5; Appendix III, Section 3.