Budget, the General Services Administration, the National Institute of Standards and Technology, and the National Telecommunications and Information Administration, provide information on computer, telecommunications, or information resources. This information includes security-related policy, regulations, standards, and guidance. A portion of the information is channelled through the senior designated official for each agency (see Federal Information Resources Management Regulation [FIRMR] Part 201-2). Agencies are expected to have mechanisms in place to distribute the information the senior designated official receives.

Computer security-related information is also available from private and federal professional societies and groups. These groups will often provide the information as a public service, although some private groups charge a fee for it. However, even for information that is free or inexpensive, the costs associated with personnel gathering the information can be high.

Internal security-related information, such as which procedures were effective, virus infections, security problems, and solutions, need to be shared within an organization. Often this information is specific to the operating environment and culture of the organization.

A computer security program administered at the organization level can provide a way to collect the internal security-related information and distribute it as needed throughout the organization. Sometimes an organization can also share this information with external groups. See Figure 6.3.

Another use of an effective conduit of information is to increase the central computer security program's ability to influence external and internal policy decisions. If the central computer security program office can represent the entire organization, then its advice is more likely to be heeded by upper management and external organizations. However, to be effective, there should be excellent communication between the system-level computer security programs and the organization level. For example, if an organization were considering consolidating its mainframes into one site (or considering distributing the processing currently done at one site), personnel at the central program could provide initial opinions about the security implications. However, to speak authoritatively, central program personnel would have to actually know the security impacts of the proposed change – information that would have to be obtained from the system-level computer security program.

Besides being able to help an organization use information more cost effectively, a computer security program can also help an organization better spend its scarce security dollars. Organizations can develop expertise and then share it, reducing the need to contract out repeatedly for similar services. The central computer security program can help facilitate information sharing.

An organization's components may develop specialized expertise, which can be shared among components. For example, one operating unit may primarily use UNIX and have developed skills in UNIX security. A second operating unit (with only one UNIX machine), may concentrate on MVS security and rely on the first unit's knowledge and skills for its UNIX machine.

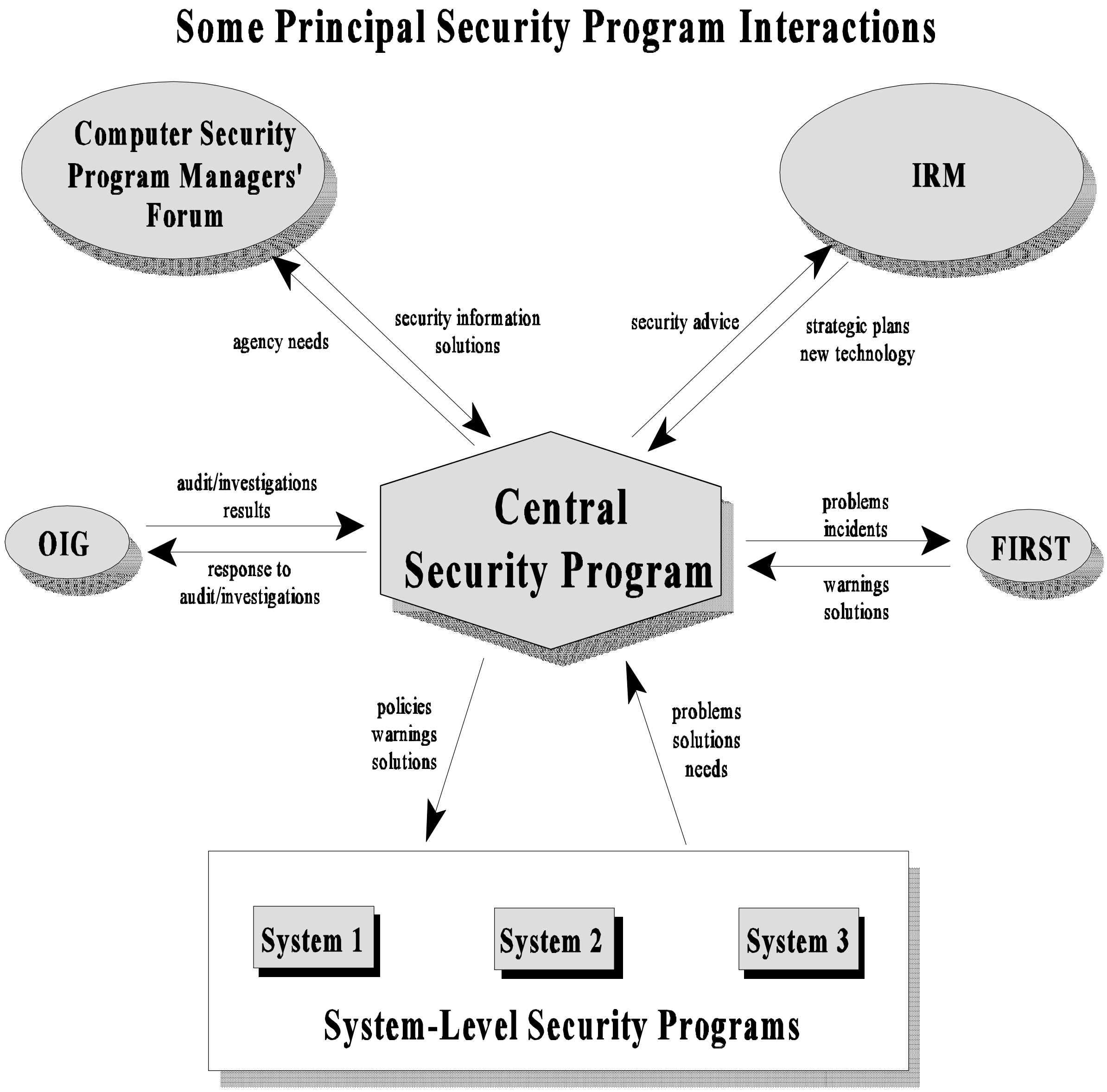

Some Principal Security Program Interactions
Computer Security Program Managers' Forum
IRM
agency needs
security information solutions
security advice
strategic plans new technology
audit/investigations results
response to audit/investigations
OIG
Central Security Program
problems incidents
warnings solutions
FIRST
policies warnings solutions
problems solutions needs
System 1
System 2
System 3
System-Level Security Programs

Figure 6.3 shows a *simplified* version of the flow of computer security-related information among various parts of an organization and across different organizations.

Figure 6.3

Personnel at the central computer security program level can also develop their own areas of expertise. For example, they could sharpen their skills could in contingency planning and risk analysis to help the entire organization perform these vital security functions.

Besides allowing an organization to share expertise and, therefore, save money, a central computer security program can use its position to consolidate requirements so the organization can negotiate discounts based on volume purchasing of security hardware and software. It also facilitates such activities as strategic planning and organizationwide incident handling and security trend analysis.

6.2.3 Central Enforcement and Oversight

Besides helping an organization improve the economy and efficiency of its computer security program, a centralized program can include an independent evaluation or enforcement function to ensure that organizational subunits are cost-effectively securing resources and following applicable policy. While the Office of the Inspector General (OIG) and external organizations, such as the General Accounting Office (GAO), also perform a valuable evaluation role, they operate outside the regular management channels. Chapters 8 and 9 further discuss the role of independent audit.

There are several reasons for having an oversight function within the regular management channel. First, computer security is an important component in the management of organizational resources. This is a responsibility that cannot be transferred or abandoned. Second, maintaining an internal oversight function allows an organization to find and correct problems without the potential embarrassment of an IG or GAO audit or investigation. Third, the organization may find different problems from those that an outside organization may find. The organization understands its assets, threats, systems, and procedures better than an external organization; additionally, people may have a tendency to be more candid with insiders.

6.3 Elements of an Effective Central Computer Security Program

For a central computer security program to be effective, it should be an established part of organization management. If system managers and applications owners do not need to consistently interact with the security program, then it can become an empty token of upper management's "commitment to security."

Stable Program Management Function. A well-established program will have a program manager recognized within the organization as the central computer security program manager. In addition, the program will be staffed with able personnel, and links will be established between the program management function and computer security personnel in other parts of the organization. A computer security program is a complex function that needs a stable base from which to direct the management of such security resources as information and money. The benefits of an oversight function cannot be achieved if the computer security program is not recognized within an organization as having expertise and authority.

Stable Resource Base. A well-established program will have a stable resource base in terms of personnel, funds, and other support. Without a stable resource base, it is impossible to plan and execute programs and projects effectively.

Existence of Policy. Policy provides the foundation for the central computer security program and is the means for documenting and promulgating important decisions about computer security. A central computer security program should also publish standards, regulations, and guidelines that implement and expand on policy. (See Chapter 5.)

Published Mission and Functions Statement. A published mission statement grounds the central computer security program into the unique operating environment of the organization. The statement clearly establishes the function of the computer security program and defines responsibilities for both the computer security program and other related programs and entities. Without such a statement, it is impossible to develop criteria for evaluating the effectiveness of the program.

Long-Term Computer Security Strategy. A well-established program explores and develops long-term strategies to incorporate computer security into the next generation of information technology. Since the computer and telecommunications field moves rapidly, it is essential to plan for future operating environments.

Compliance Program. A central computer security program needs to address compliance with national policies and requirements, as well as organization-specific requirements. National requirements include those prescribed under the Computer Security Act of 1987, OMB Circular A-130, the FIRMR, and Federal Information Processing Standards.

Intraorganizational Liaison. Many offices within an organization can affect computer security. The Information Resources Management organization and physical security office are two obvious examples. However, computer security often overlaps with other offices, such as safety, reliability and quality assurance, internal control, or the Office of the Inspector General. An effective program should have established relationships with these groups in order to integrate computer security into the organization's management. The relationships should encompass more than just the sharing of information; the offices should influence each other.

Example

Agency IRM offices engage in strategic and tactical planning for both information and information technology, in accordance with the Paperwork Reduction Act and OMB Circular A-130. Security should be an important component of these plans. The security needs of the agency should be reflected in the information technology choices and the information needs of the agency should be reflected in the security program.

Liaison with External Groups. There are many sources of computer security information, such as

NIST's Computer Security Program Managers' Forum, computer security clearinghouse, and the Forum of Incident Response and Security Teams (FIRST). An established program will be knowledgeable of and will take advantage of external sources of information. It will also be a provider of information.

6.4 System-Level Computer Security Programs

While the central program addresses the entire spectrum of computer security for an organization, system-level programs ensure appropriate and cost-effective security for each system.[59] This includes influencing decisions about what controls to implement, purchasing and installing technical controls, day-to-day computer security administration, evaluating system vulnerabilities, and responding to security problems. It encompasses all the areas discussed in the handbook.

System-level computer security program personnel are the local advocates for computer security. The system security manager/officer raises the issue of security with the cognizant system manager and helps develop solutions for security problems. For example, has the application owner made clear the system's security requirements? Will bringing a new function online affect security, and if so, how? Is the system vulnerable to hackers and viruses? Has the contingency plan been tested? Raising these kinds of questions will force system managers and application owners to identify and address their security requirements.

6.5 Elements of Effective System-Level Programs

Like the central computer security program, many factors influence how successful a system-level computer security program is. Many of these are similar to the central program. This section addresses some additional considerations.

Security Plans. The Computer Security Act mandates that agencies develop computer security and privacy plans for sensitive systems. These plans ensure that each federal and federal interest system has appropriate and cost-effective security. System-level security personnel should be in a position to develop and implement security plans. Chapter 8 discusses the plans in more detail.

System-Specific Security Policy. Many computer security policy issues need to be addressed on a system-specific basis. The issues can vary for each system, although access control and the designation of personnel with security responsibility are likely to be needed for all systems. A cohesive and comprehensive set of security policies can be developed by using a process that

[59] As is implied by the name, an organization will typically have several system-level computer security programs. In setting up these programs, the organization should carefully examine the scope of each system-level program. System-level computer security programs may address, for example, the computing resources within an operational element, a major application, or a group of similar systems (either technologically or functionally).

derives security rules from security goals, as discussed in Chapter 5.

Life Cycle Management. As discussed in Chapter 8, security must be managed throughout a system's life cycle. This specifically includes ensuring that changes to the system are made with attention to security and that accreditation is accomplished.

Integration With System Operations. The system-level computer security program should consist of people who understand the system, its mission, its technology, and its operating environment. Effective security management usually needs to be integrated into the management of the system. Effective integration will ensure that system managers and application owners consider security in the planning and operation of the system. The system security manager/officer should be able to participate in the selection and implementation of appropriate technical controls and security procedures and should understand system vulnerabilities. Also, the system-level computer security program should be capable of responding to security problems in a timely manner.

For large systems, such as a mainframe data center, the security program will often include a manager and several staff positions in such areas as access control, user administration, and contingency and disaster planning. For small systems, such as an officewide local-area-network (LAN), the LAN administrator may have adjunct security responsibilities.

Separation From Operations. A natural tension often exists between computer security and operational elements. In many instances, operational components -- which tend to be far larger and therefore more influential -- seek to resolve this tension by embedding the computer security program in computer operations. The typical result of this organizational strategy is a computer security program that lacks independence, has minimal authority, receives little management attention, and has few resources. As early as 1978, GAO identified this organizational mode as one of the principal basic weaknesses in federal agency computer security programs.[60] System-level programs face this problem most often.

This conflict between the need to be a part of system management and the need for independence has several solutions. The basis of many of the solutions is a link between the computer security program and upper management, often through the central computer security program. A key requirement of this setup is the existence of a reporting structure that does not include system management. Another possibility is for the computer security program to be completely independent of system management and to report directly to higher management. There are many hybrids and permutations, such as co-location of computer security and systems management staff but separate reporting (and supervisory) structures. Figure 6.4 presents *one example* of

[60] General Accounting Office, "Automated System Security -- Federal Agencies Should Strengthen Safeguards Over Personal and Other Sensitive Data," GAO Report LCD 78-123, Washington, DC, 1978.

Example of Organizational Placement of Computer Security Functions

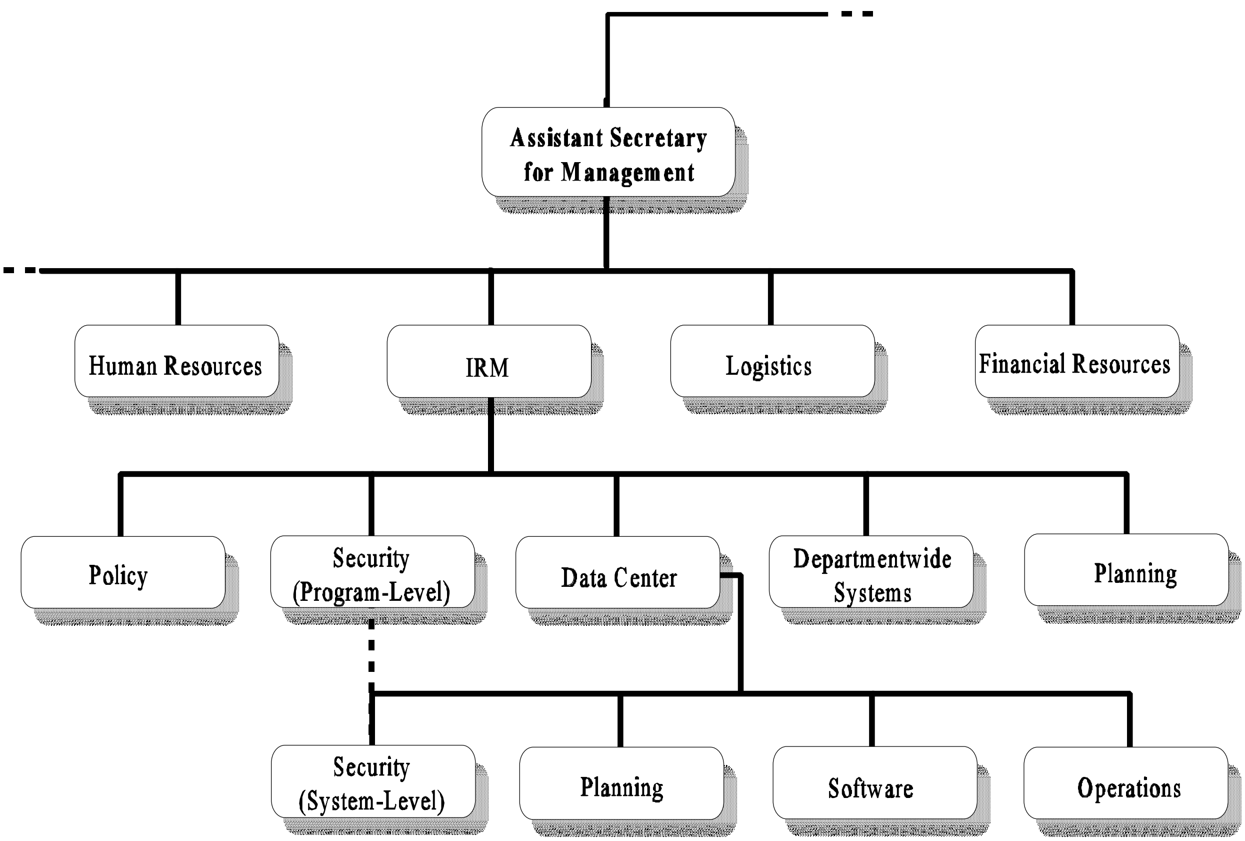


Figure 6.4 illustrates one example of the placement of the computer security program-level and system-level functions. The program-level function is located within the IRM organization and sets policy for the organization as a whole. The system-level function, located within the Data Center, provides for day-to-day security at that site. Note that, although not pictured, other system-level programs may exist for other facilities (e.g., under another Assistant Secretary).

Figure 6.4

placement of the computer security program within a typical Federal agency.[61]

[61] No implication that this structure is ideal is intended.

6.6 Central and System-Level Program Interactions

A system-level program that is not integrated into the organizational program may have difficulty influencing significant areas affecting security. The system-level computer security program implements the policies, guidance, and regulations of the central computer security program. The system-level office also learns from the information disseminated by the central program and uses the experience and expertise of the entire organization. The system-level computer security program further distributes information to systems management as appropriate.

Communications, however, should not be just one way. System-level computer security programs inform the central office about their needs, problems, incidents, and solutions. Analyzing this information allows the central computer security program to represent the various systems to the organization's management and to external agencies and advocate programs and policies beneficial to the security of all the systems.

6.7 Interdependencies

The general purpose of the computer security program, to improve security, causes it to overlap with other organizational operations as well as the other security controls discussed in the handbook. The central or system computer security program will address most controls at the policy, procedural, or operational level.

Policy. Policy is issued to establish the computer security program. The central computer security program(s) normally produces policy (and supporting procedures and guidelines) concerning general and organizational security issues and often issue-specific policy. However, the system-level computer security program normally produces policy for that system. Chapter 5 provides additional guidance.

Life Cycle Management. The process of securing a system over its life cycle is the role of the system-level computer security program. Chapter 8 addresses these issues.

Independent Audit. The independent audit function described in Chapters 8 and 9 should complement a central computer security program's compliance functions.

6.8 Cost Considerations

This chapter discussed how an organizationwide computer security program can manage security resources, including financial resources, more effectively. The cost considerations for a system-level computer security program are more closely aligned with the overall cost savings in having security.

The most significant direct cost of a computer security program is personnel. In addition, many programs make frequent and effective use of consultants and contractors. A program also needs funds for training and for travel, oversight, information collection and dissemination, and meetings with personnel at other levels of computer security management.

References

Federal Information Resources Management Regulations, especially 201-2. General Services Administration. Washington, DC.

General Accounting Office. *Automated Systems Security–Federal Agencies Should Strengthen Safeguards Over Personal and Other Sensitive Data*. GAO Report LCD 78-123. Washington, DC. 1978.

General Services Administration. *Information Resources Security: What Every Federal Manager Should Know*. Washington, DC.

Helsing, C., M. Swanson, and M. Todd. *Executive Guide to the Protection of Information Resources.*, Special Publication 500-169. Gaithersburg, MD: National Institute of Standards and Technology, 1989.

Helsing, C., M. Swanson, and M. Todd. *Management Guide for the Protection of Information Resources.* Special Publication 500-170. Gaithersburg, MD: National Institute of Standards and Technology, 1989.

"Managing an Organization Wide Security Program." Computer Security Institute, San Francisco, CA. (course)

Office of Management and Budget. "Guidance for Preparation of Security Plans for Federal Computer Systems That Contain Sensitive Information." OMB Bulletin 90-08. Washington, DC, 1990.

Office of Management and Budget. *Management of Federal Information Resources*. OMB Circular A-130.

Owen, R., Jr. "Security Management: Using the Quality Approach." *Proceedings of the 15th National Computer Security Conference*. Baltimore, MD: Vol. 2, 1992. pp. 584-592.

Spiegel, L. "Good LAN Security Requires Analysis of Corporate Data." *Infoworld*. 15(52), 1993. p. 49.

II. Management Controls

U.S. Congress. *Computer Security Act of 1987*. Public Law 100-235. 1988.

Chapter 7

COMPUTER SECURITY RISK MANAGEMENT

Risk is the possibility of something adverse happening. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk. Though perhaps not always aware of it, individuals manage risks every day. Actions as routine as buckling a car safety belt, carrying an umbrella when rain is forecast, or writing down a list of things to do rather than trusting to memory fall into the purview of risk management. People recognize various threats to their best interests and take precautions to guard against them or to minimize their effects.

Both government and industry routinely manage a myriad of risks. For example, to maximize the return on their investments, businesses must often decide between aggressive (but high-risk) and slow-growth (but more secure) investment plans. These decisions require analysis of risk, relative to potential benefits, consideration of alternatives, and, finally, implementation of what management determines to be the best course of action.

> Management is concerned with many types of risk. Computer security risk management addresses risks which arise from an organization's use of information technology.

While there are many models and methods for risk management, there are several basic activities and processes that should be performed. In discussing risk management, it is important to recognize its basic, most fundamental assumption: computers cannot ever be fully secured. There is always risk, whether it is from a trusted employee who defrauds the system or a fire that destroys critical resources. Risk management is made up of two primary and one underlying activities; risk assessment and risk mitigation are the primary activities and uncertainty analysis is the underlying one.

> Risk assessment often produces an important side benefit -- indepth knowledge about a system and an organization as risk analysts try to figure out how systems and functions are interrelated.

7.1 Risk Assessment

Risk assessment, the process of analyzing and interpreting risk, is comprised of three basic activities: (1) determining the assessment's scope and methodology; (2) collecting and analyzing data; and 3) interpreting the risk analysis results.[62]

7.1.1 Determining the Assessment's Scope and Methodology

The first step in assessing risk is to identify the system under consideration, the part of the system that will be analyzed, and the analytical method including its level of detail and formality.

A risk assessment can focus on many different areas such as: technical and operational controls to be designed into a new application, the use of telecommunications, a data center, or an entire organization.

The assessment may be focused on certain areas where either the degree of risk is unknown or is known to be high. Different parts of a system may be analyzed in greater or lesser detail. Defining the scope and boundary can help ensure a cost-effective assessment. Factors that influence scope include what phase of the life cycle a system is in: more detail might be appropriate for a new system being developed than for an existing system undergoing an upgrade. Another factor is the relative importance of the system under examination: the more essential the system, the more thorough the risk analysis should be. A third factor may be the magnitude and types of changes the system has undergone since the last risk analysis. The addition of new interfaces would warrant a different scope than would installing a new operating system.

Methodologies can be formal or informal, detailed or simplified, high or low level, quantitative (computationally based) or qualitative (based on descriptions or rankings), or a combination of these. No single method is best for all users and all environments.

How the boundary, scope, and methodology are defined will have major consequences in terms of (1) the total amount of effort spent on risk management and (2) the type and usefulness of the assessment's results. The boundary and scope should be selected in a way that will produce an outcome that is clear, specific, and useful to the system and environment under scrutiny.

7.1.2 Collecting and Analyzing Data

Good documentation of risk assessments will make later risk assessments less time consuming and, if a question arises, will help explain why particular security decisions were made.

Risk has many different components: assets, threats, vulnerabilities, safeguards, consequences, and likelihood. This examination normally includes gathering data about the threatened area *and* synthesizing

[62] Many different terms are used to describe risk management and its elements. The definitions used in this paper are based on the NIST Risk Management Framework.

and analyzing the information to make it useful.

Because it is possible to collect much more information than can be analyzed, steps need to be taken to limit information gathering and analysis. This process is called *screening*. A risk management effort should focus on those areas that result in the greatest consequence to the organization (i.e., can cause the most harm). This can be done by ranking threats and assets.

A risk management methodology does not necessarily need to analyze each of the components of risk separately. For example, assets/consequences or threats/likelihoods may be analyzed together.

Asset Valuation. These include the information, software, personnel, hardware, and physical assets (such as the computer facility). The value of an asset consists of its intrinsic value and the near-term impacts and long-term consequences of its compromise.

Consequence Assessment. The consequence assessment estimates the degree of harm or loss that could occur. *Consequences* refers to the overall, aggregate harm that occurs, not just to the near-term or immediate impacts. While such impacts often result in disclosure, modification, destruction, or denial of service, consequences are the more significant long-term effects, such as lost business, failure to perform the system's mission, loss of reputation, violation of privacy, injury, or loss of life. The more severe the consequences of a threat, the greater the risk to the system (and, therefore, the organization).

Threat Identification. A threat is an entity or event with the potential to harm the system. Typi cal threats are errors, fraud, disgruntled employees, fires, water damage, hackers, and viruses. Threats should be identified and analyzed to determine the likelihood of their occurrence and their potential to harm assets.

In addition to looking at "big-ticket" threats, the risk analysis should investigate areas that are poorly understood, new, or undocumented. If a facility has a well-tested physical access control system, less effort to identify threats may be warranted for it than for unclear, untested software backup procedures.

The risk analysis should concentrate on those threats most likely to occur and affect important assets. In some cases, determining which threats are realistic is not possible until after the threat analysis is begun. Chapter 4 provides additional discussion of today's most prevalent threats.

Safeguard Analysis. A safeguard is any action, device, procedure, technique, or other measure that reduces a system's vulnerability to a threat. Safeguard analysis should include an examination of the effectiveness of the existing security measures. It can also identify new safeguards that could be implemented in the system; however, this is normally performed later in the risk management process.

Vulnerability Analysis. A vulnerability is a condition or weakness in (or absence of) security procedures, technical controls, physical controls, or other controls that could be exploited by a threat. Vulnerabilities are often analyzed in terms of missing safeguards. Vulnerabilities contribute to risk because they may "allow" a threat to harm the system.

The interrelationship of vulnerabilities, threats, and assets is critical to the analysis of risk. Some of these interrelationships are pictured in Figure 7.1. However, there are other interrelationships such as the presence of a vulnerability inducing a threat. (For example, a normally honest employee might be tempted to alter data when the employee sees that a terminal has been left logged on.)

Threats, Vulnerabilities, Safeguards, and Assets

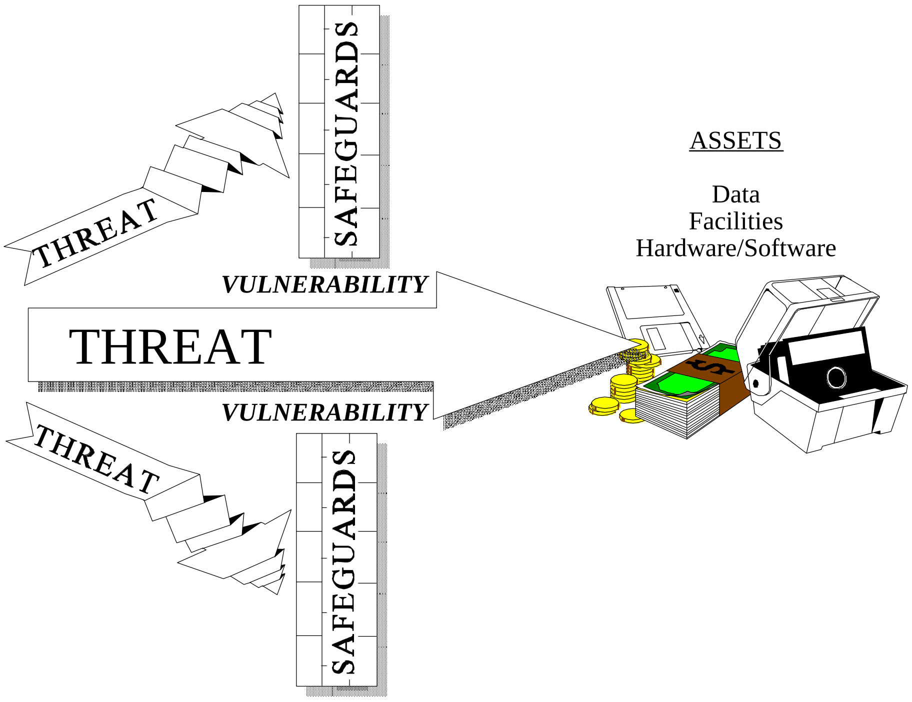


Figure 7.1 Safeguards prevent threats from harming assets. However, if an appropriate safeguard is not present, a vulnerability exists which can be exploited by a threat, thereby puttting assets at risk.

Figure 7.1

Likelihood Assessment. Likelihood is an estimation of the frequency or chance of a threat happening. A likelihood assessment considers the presence, tenacity, and strengths of threats as well as the effectiveness of safeguards (or presence of vulnerabilities). In general, historical information about many threats is weak, particularly with regard to human threats; thus, experience in this area is important. Some threat data -- especially on physical threats such as fires or floods -- is stronger. Care needs to be taken in using any statistical threat data; the source of the data or the analysis may be inaccurate or incomplete. In general, the greater the likelihood of a threat occurring, the greater the risk.

7.1.3 Interpreting Risk Analysis Results[63]

The risk assessment is used to support two related functions: the acceptance of risk and the selection of cost-effective controls. To accomplish these functions, the risk assessment must produce a meaningful output that reflects what is truly important to the organization. Limiting the risk interpretation activity to the most significant risks is another way that the risk management process can be focused to reduce the overall effort while still yielding useful results.

If risks are interpreted consistently across an organization, the results can be used to prioritize systems to be secured.

Risk Analysis Results

Risk analysis results are typically represented quantitatively and/or qualitatively. Quantitative measures may be expressed in terms of reduced expected monetary losses, such as annualized loss expectancies or single occurrences of loss. Qualitative measures are descriptive, expressed in terms such as high, medium, or low, or rankings on a scale of 1 to 10.

Risk management can *help* a manager select the most appropriate controls; however, it is not a magic wand that instantly eliminates all difficult issues. The quality of the output depends on the quality of the input and the type of analytical methodology used. In some cases, the amount of work required to achieve high-quality input will be too costly. In other cases, achieving high-quality input may be impossible, especially for such variables as the prevalence of a particular threat or the anticipated effectiveness of a proposed safeguard. For all practical purposes, complete information is never available; uncertainty is always present. Despite these drawbacks, risk management provides a very powerful tool for analyzing the risk associated with computer systems.

7.2 Risk Mitigation

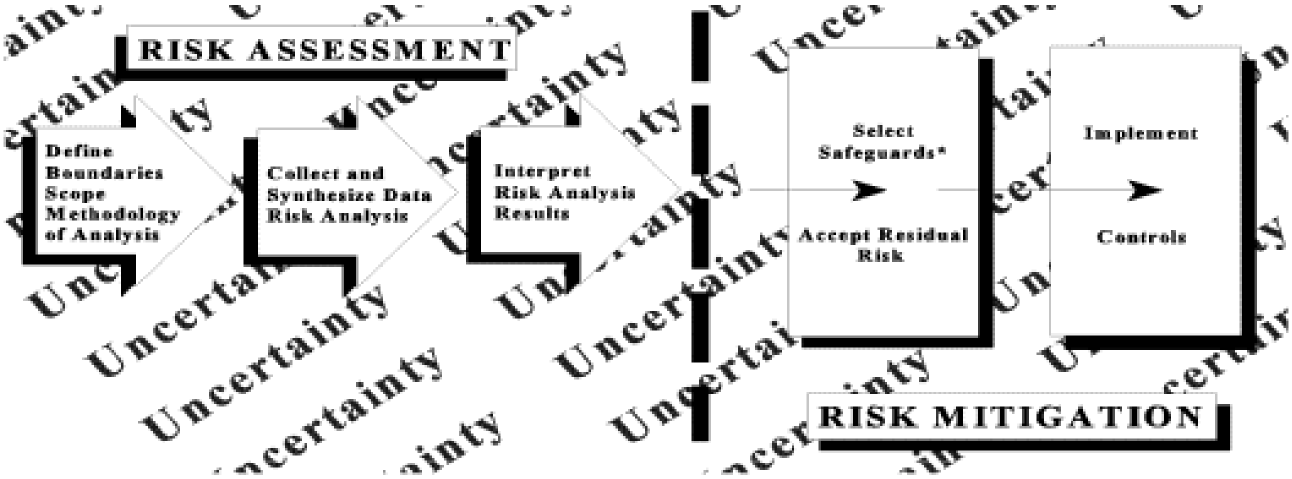
Risk mitigation involves the selection and implementation of security controls to reduce risk to a level acceptable to management, within applicable constraints. Although there is flexibility in how risk assessment is conducted, the sequence of identifying boundaries, analyzing input, and producing an output is quite natural. The process of risk mitigation has greater flexibility, and the sequence will differ more, depending on organizational culture and the purpose of the risk management

[63] The NIST Risk Management Framework refers to risk interpretation as risk measurement. The term "interpretation" was chosen to emphasize the wide variety of possible outputs from a risk assessment.

II. Management Controls

activity. Although these activities are discussed

How Risk Management Works



* There are many possible approaches to safeguard selection. Some involve looping back and reexamining risk analysis data.

Figure 7.2 shows the flow of risk management activities and processes. A major division in risk management (shown by the verticle line) is between risk assessment and risk mitigation. Both are critical parts of the risk management process. Uncertainty is always present.

Figure 7.2

in a specific sequence, they need not be performed in that sequence. In particular, the selection of safeguards and risk acceptance testing are likely to be performed simultaneously.[64]

[64] This is often viewed as a circular, iterative process.

7.2.1 Selecting Safeguards

A primary function of computer security risk management is the identification of appropriate controls. In designing (or reviewing) the security of a system, it may be obvious that some controls should be added (e.g., because they are required by law or because they are clearly cost-effective). It may also be just as obvious that other controls may be too expensive (considering both monetary and nonmonetary factors). For example, it may be immediately apparent to a manager that closing and locking the door to a particular room that contains local area network equipment is a needed control, while posting a guard at the door would be too expensive and not user-friendly.

In every assessment of risk, there will be many areas for which it will not be obvious what kind of controls are appropriate. Even considering only monetary issues, such as whether a control would cost more than the loss it is supposed to prevent, the selection of controls is not simple. However, in selecting appropriate controls, managers need to consider many factors, including:

- organizational policy, legislation, and regulation;
- safety, reliability, and quality requirements;
- system performance requirements;
- timeliness, accuracy, and completeness requirements;
- the life cycle costs of security measures;
- technical requirements; and
- cultural constraints.

What Is a *What If* Analysis?

A *what if* analysis looks at the costs and benefits of various combinations of controls to determine the optimal combination for a particular circumstance. In this simple example (which addresses only one control), suppose that hacker break-ins alert agency computer security personnel to the security risks of using passwords. They may wish to consider replacing the password system with stronger identification and authentication mechanisms, or just strengthening their password procedures. First, the **status quo** is examined. The system in place puts minimal demands upon users and system administrators, but the agency has had three hacker break-ins in the last six months.

What if passwords are strengthened? Personnel may be required to change passwords more frequently or may be required to use a numeral or other nonalphabetic character in their password. There are no direct monetary expenditures, but staff and administrative overhead (e.g., training and replacing forgotten passwords) is increased. Estimates, however, are that this will reduce the number of successful hacker break-ins to three or four per year.

What if stronger identification and authentication technology is used? The agency may wish to implement stronger safeguards in the form of one-time cryptographic-based passwords so that, even if a password were obtained, it would be useless. Direct costs may be estimated at $45,000, and yearly recurring costs at $8,000. An initial training program would be required, at a cost of $17,500. The agency estimates, however, that this would prevent virtually all break-ins.

Computer security personnel use the results of this analysis to make a recommendation to their management officer, who then weighs the costs and benefits, takes into account other constraints (e.g., budget), and selects a solution.

One method of selecting safeguards uses a "what if" analysis. With this method, the effect of adding various safeguards (and, therefore, reducing vulnerabilities) is tested to see what difference each makes with regard to cost, effectiveness, and other relevant factors, such as those listed above. Trade-offs among the factors can be seen. The analysis of trade-offs also supports the acceptance of residual risk, discussed below. This method typically involves multiple iterations of the risk analysis to see how the proposed changes affect the risk analysis result.

Another method is to categorize types of safeguards and recommend implementing them for various levels of risk. For example, stronger controls would be implemented on high-risk systems than on low-risk systems. This method normally does not require multiple iterations of the risk analysis.

As with other aspects of risk management, screening can be used to concentrate on the highest-risk areas. For example once could focus on risks with very severe consequences, such as a very high dollar loss or loss of life or on the threats that are most likely to occur.

7.2.2 Accept Residual Risk

At some point, management needs to decide if the operation of the computer system is acceptable, given the kind and severity of remaining risks. Many managers do not fully understand computer-based risk for several reasons: (1) the type of risk may be different from risks previously associated with the organization or function; (2) the risk may be technical and difficult for a lay person to understand, or (3) the proliferation and decentralization of computing power can make it difficult to identify key assets that may be at risk.

Risk acceptance, like the selection of safeguards, should take into account various factors besides those addressed in the risk assessment. In addition, risk acceptance should take into account the limitations of the risk assessment. (See the section below on uncertainty.) Risk acceptance is linked to the selection of safeguards since, in some cases, risk may have to be accepted because safeguards are too expensive (in either monetary or nonmonetary factors).

Within the federal government, the acceptance of risk is closely linked with the authorization to use a computer system, often called *accreditation*, discussed in Chapters 8 and 9. Accreditation is the acceptance of risk by management resulting in a formal approval for the system to become operational or remain so. As discussed earlier in this chapter, one of the two primary functions of risk management is the interpretation of risk for the purpose of risk acceptance.

7.2.3 Implementing Controls and Monitoring Effectiveness

Merely selecting appropriate safeguards does not reduce risk; those safeguards need to be effectively implemented. Moreover, to continue to be effective, risk management needs to be an ongoing process. This requires a periodic assessment and improvement of safeguards and reanalysis of risks. Chapter 8 discusses how periodic risk assessment is an integral part of the overall management of a system. (See especially the diagram on page 83.)

The risk management process normally produces security requirements that are used to design, purchase, build, or otherwise obtain safeguards or implement system changes. The integration of risk management into the life cycle process is discussed in Chapter 8.

7.3 Uncertainty Analysis

Risk management often must rely on speculation, best guesses, incomplete data, and many unproven assumptions. The uncertainty analysis attempts to document this so that the risk management results can be used knowledgeably. There are two primary sources of uncertainty in the risk management process: (1) a lack of confidence or precision in the risk management model or methodology and (2) a lack of sufficient information to determine the exact value of the elements of the risk model, such as threat frequency, safeguard effectiveness, or consequences.

> While uncertainty is always present it should not invalidate a risk assessment. Data and models, while imperfect, can be good enough for a given purpose.

The risk management framework presented in this chapter is a generic description of risk management elements and their basic relationships. For a methodology to be useful, it should further refine the relationships and offer some means of screening information. In this process, assumptions may be made that do not accurately reflect the user's environment. This is especially evident in the case of safeguard selection, where the number of relationships among assets, threats, and vulnerabilities can become unwieldy.

The data are another source of uncertainty. Data for the risk analysis normally come from two sources: statistical data and expert analysis. Statistics and expert analysis can sound more authoritative than they really are. There are many potential problems with statistics. For example, the sample may be too small, other parameters affecting the data may not be properly accounted for, or the results may be stated in a misleading manner. In many cases, there may be insufficient data. When expert analysis is used to make projections about future events, it should be recognized that the projection is subjective and is based on assumptions made (but not always explicitly articulated) by the expert.

7.4 Interdependencies

Risk management touches on every control and every chapter in this handbook. It is, however, most closely related to life cycle management and the security planning process. The requirement to perform risk management is often discussed in organizational policy and is an issue for organizational oversight. These issues are discussed in Chapters 5 and 6.

7.5 Cost Considerations

The building blocks of risk management presented in this chapter can be used creatively to develop methodologies that concentrate expensive analysis work where it is most needed. Risk management can become expensive very quickly if an expansive boundary and detailed scope are selected. It is very important to use screening techniques, as discussed in this chapter, to limit the overall effort. The goals of risk management should be kept in mind as a methodology is selected or developed. The methodology should concentrate on areas where identification of risk and the selection of cost-effective safeguards are needed.

The cost of different methodologies can be significant. A "back-of-the-envelope" analysis or high-medium-low ranking can often provide all the information needed. However, especially for the selection of expensive safeguards or the analysis of systems with unknown consequences, more in-depth analysis may be warranted.

References

Caelli, William, Dennis Longley, and Michael Shain. *Information Security Handbook*. New York, NY: Stockton Press, 1991.

Carroll, J.M. *Managing Risk: A Computer-Aided Strategy.* Boston, MA: Butterworths 1984.

Gilbert, Irene. *Guide for Selecting Automated Risk Analysis Tools*. Special Publication 500-174. Gaithersburg, MD: National Institute of Standards and Technology, October 1989.

Jaworski, Lisa. "Tandem Threat Scenarios: A Risk Assessment Approach." *Proceedings of the 16th National Computer Security Conference*, Baltimore, MD: Vol. 1, 1993. pp. 155-164.

Katzke, Stuart. "A Framework for Computer Security Risk Management." *8th Asia Pacific Information Systems Control Conference Proceedings*. EDP Auditors Association, Inc., Singapore, October 12-14, 1992.

Levine, M. "Audit Serve Security Evaluation Criteria." *Audit Vision*. 2(2), 1992. pp. 29-40.

National Bureau of Standards. *Guideline for Automatic Data Processing Risk Analysis*. Federal Information Processing Standard Publication 65. August 1979.

National Institute of Standards and Technology. *Guideline for the Analysis of Local Area Network Security*. Federal Information Processing Standard Publication 191. November 1994.

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.

Proceedings, 4th International Computer Security Risk Management Model Builders Workshop. University of Maryland, National Institute of Standards and Technology, College Park, MD, August 6-8, 1991.

Proceedings, 3rd International Computer Security Risk Management Model Builders Workshop, Los Alamos National Laboratory, National Institute of Standards and Technology, National Computer Security Center, Santa Fe, New Mexico, August 21-23, 1990.

Proceedings, 1989 Computer Security Risk Management Model Builders Workshop, AIT Corporation, Communications Security Establishment, National Computer Security Center, National Institute of Standards and Technology, Ottawa, Canada, June 20-22, 1989.

Proceedings, 1988 Computer Security Risk Management Model Builders Workshop, Martin Marietta, National Bureau of Standards, National Computer Security Center, Denver, Colorado, May 24-26, 1988.

Spiegel, L. "Good LAN Security Requires Analysis of Corporate Data." *Infoworld*. 15(52), 1993. p. 49.

Wood, C. "Building Security Into Your System Reduces the Risk of a Breach." *LAN Times*. 10(3), 1993. p. 47.

Wood C., et al., *Computer Security: A Comprehensive Controls Checklist*. New York, NY: John Wiley & Sons, 1987.

Chapter 8

SECURITY AND PLANNING IN THE COMPUTER SYSTEM LIFE CYCLE

Like other aspects of information processing systems, security is most effective and efficient if planned and managed throughout a computer system's life cycle, from initial planning, through design, implementation, and operation, to disposal.[65] Many security-relevant events and analyses occur during a system's life. This chapter explains the relationship among them and how they fit together.[66] It also discusses the important role of security planning in helping to ensure that security issues are addressed comprehensively.

This chapter examines:

- system security plans,
- the components of the computer system life cycle,
- the benefits of integrating security into the computer system life cycle, and
- techniques for addressing security in the life cycle.

8.1 Computer Security Act Issues for Federal Systems

Planning is used to help ensure that security is addressed in a comprehensive manner throughout a system's life cycle. For federal systems, the Computer Security Act of 1987 sets forth a statutory requirement for the preparation of computer security plans for all sensitive systems.[67] The intent and spirit of the Act is to improve computer security in the federal government, not to create paperwork. In keeping with this intent, the Office of Management and Budget (OMB) and NIST have guided agencies toward a planning process that emphasizes good planning and management of computer security within an agency and for each computer system. As emphasized in this

[65] A computer system refers to a collection of processes, hardware, and software that perform a function. This includes applications, networks, or support systems.

[66] Although this chapter addresses a life cycle process that starts with system initiation, the process can be initiated at any point in the life cycle.

[67] An organization will typically have many computer security plans. However, it is not necessary that a separate and distinct plan exist for every physical system (e.g., PCs). Plans may address, for example, the computing resources within an operational element, a major application, or a group of similar systems (either technologically or functionally).

chapter, computer *security* management should be a part of computer *systems* management. The benefit of having a distinct computer security plan is to ensure that computer security is not overlooked.

The Act required the submission of plans to NIST and the National Security Agency (NSA) for review and comment, a process which has been completed. Current guidance on implementing the Act requires agencies to obtain independent review of computer security plans. This review may be internal or external, as deemed appropriate by the agency.

"The purpose of the system security plan is to provide a basic overview of the security and privacy requirements of the subject system and the agency's plan for meeting those requirements. The system security plan may also be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system."

- OMB Bulletin 90-08

A "typical" plan briefly describes the important security considerations for the system and provides references to more detailed documents, such as system security plans, contingency plans, training programs, accreditation statements, incident handling plans, or audit results. This enables the plan to be used as a management tool without requiring repetition of existing documents. For smaller systems, the plan may include all security documentation. As with other security documents, if a plan addresses specific vulnerabilities or other information that could compromise the system, it should be kept private. It also has to be kept up-to-date.

8.2 Benefits of Integrating Security in the Computer System Life Cycle

Different people can provide security input throughout the life cycle of a system, including the accrediting official, data users, systems users, and system technical staff.

Although a computer security plan can be developed for a system at any point in the life cycle, the recommended approach is to draw up the plan at the beginning of the computer system life cycle. Security, like other aspects of a computer system, is best managed if planned for throughout the computer system life cycle. It has long been a tenet of the computer community that it costs ten times more to add a feature in a system *after* it has been designed than to include the feature in the system at the initial design phase. The principal reason for implementing security during a system's development is that it is more difficult to implement it later (as is usually reflected in the higher costs of doing so). It also tends to disrupt ongoing operations.
Security also needs to be incorporated into the later phases of the computer system life cycle to help ensure that security keeps up with changes in the system's environment, technology, procedures, and personnel. It also ensures that security is considered in system upgrades, including the purchase of new components or the design of new modules. Adding new security

controls to a system after a security breach, mishap, or audit can lead to haphazard security that can be more expensive and less effective that security that is already integrated into the system. It can also significantly degrade system performance. Of course, it is virtually impossible to anticipate the whole array of problems that may arise during a system's lifetime. Therefore, it is generally useful to update the computer security plan at least at the end of each phase in the life cycle and after each re-accreditation. For many systems, it may be useful to update the plan more often.

Life cycle management also helps document security-relevant decisions, in addition to helping assure management that security is fully considered in all phases. This documentation benefits system management officials as well as oversight and independent audit groups. System management personnel use documentation as a self-check and reminder of why decisions were made so that the impact of changes in the environment can be more easily assessed. Oversight and independent audit groups use the documentation in their reviews to verify that system management has done an adequate job and to highlight areas where security may have been overlooked. This includes examining whether the documentation accurately reflects how the system is actually being operated.

Within the federal government, the Computer Security Act of 1987 and its implementing instructions provide specific requirements for computer security plans. These plans are a form of documentation that helps ensure that security is considered not only during system design and development but also throughout the rest of the life cycle. Plans can also be used to be sure that requirements of Appendix III to OMB Circular A-130, as well as other applicable requirements, have been addressed.

8.3 Overview of the Computer System Life Cycle

There are many models for the computer system life cycle but most contain five basic phases, as pictured in Figure 8.1.

- *Initiation*. During the initiation phase, the need for a system is expressed and the purpose of the system is documented.

- *Development/Acquisition*. During this phase the system is designed, purchased, programmed, developed, or otherwise constructed. This phase often consists of other defined cycles, such as the system development cycle or the acquisition cycle.

- *Implementation*. After initial system testing, the system is installed or fielded.

- *Operation/Maintenance*. During this phase the system performs its work. The system is almost always modified by the addition of hardware and software and by numerous other events.

- *Disposal*. The computer system is disposed of once the transition to a new computer system is completed.

Each phase can apply to an entire system, a new component or module, or a system upgrade. As with other aspects of systems management, the level of detail and analysis for each activity described here is determined by many factors including size, complexity, system cost, and sensitivity.

Many different "life cycles" are associated with computer systems, including the system development, acquisition, and information life cycles.

Many people find the concept of a computer system life cycle confusing because many cycles occur within the broad framework of the *entire* computer system life cycle. For example, an organization could develop a system, using a system *development* life cycle. During the system's life, the organization might purchase new components, using the *acquisition* life cycle.

Moreover, the computer system life cycle itself is merely one component of other life cycles. For example, consider the *information life cycle*. Normally information, such as personnel data, is used much longer than the life of one computer system. If an employee works for an organization for thirty years and collects retirement for another twenty, the employee's automated personnel record will probably pass through many different organizational computer systems owned by the company. In addition, parts of the information will also be used in other computer systems, such as those of the Internal Revenue Service and the Social Security Administration.

8.4 Security Activities in the Computer System Life Cycle[68]

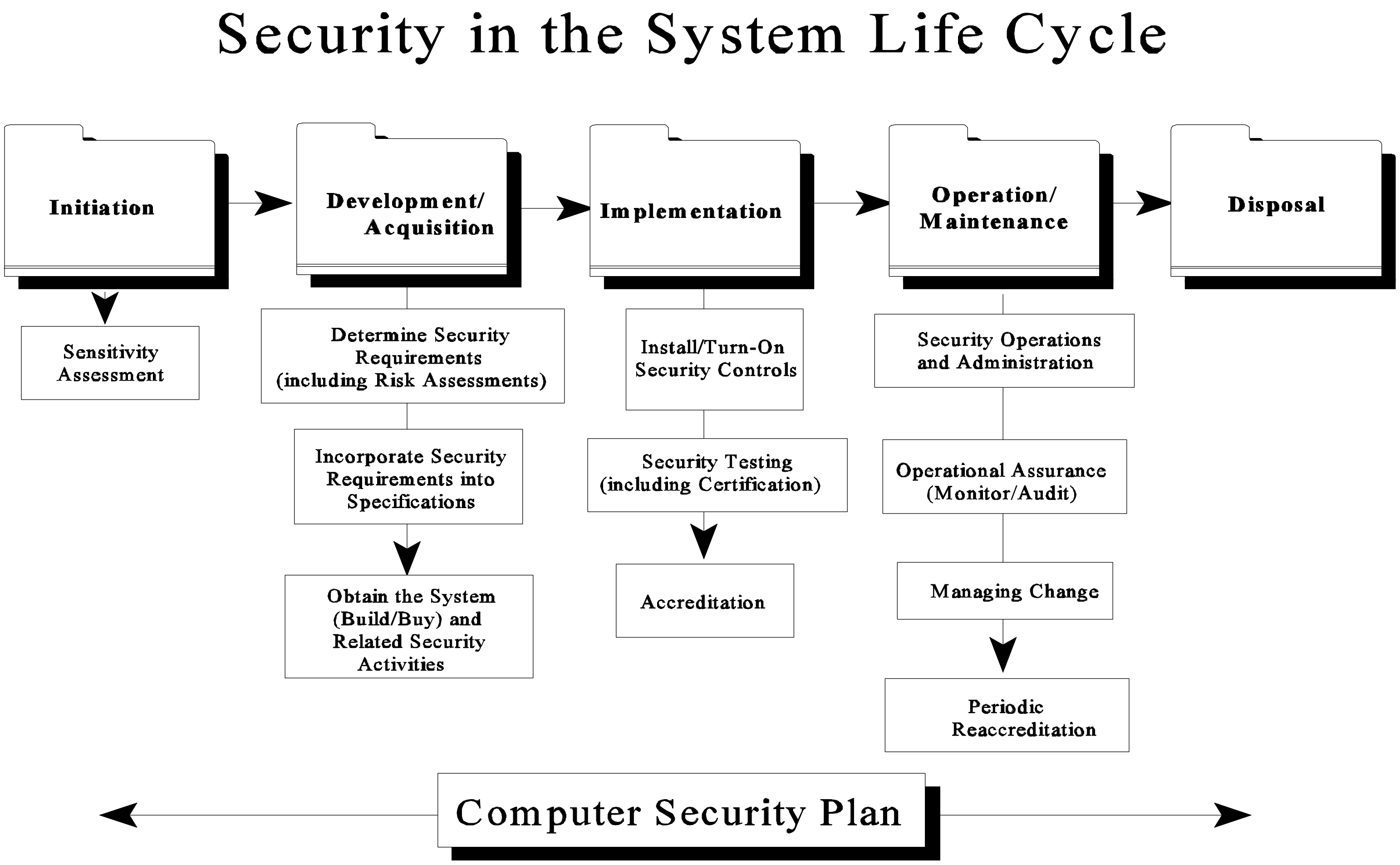
This section reviews the security activities that arise in each stage of the computer system life cycle. (See Figure 8.1.)

8.4.1 Initiation

The conceptual and early design process of a system involves the discovery of a need for a new system or enhancements to an existing system; early ideas as to system characteristics and proposed functionality; brainstorming sessions on architectural, performance, or functional system aspects; and environmental, financial, political, or other constraints. At the same time, the basic *security* aspects of a system should be developed along with the early system design. This can be

[68] For brevity and because of the uniqueness of each system, none of these discussions can include the details of all possible security activities at any particular life cycle phase.

done through a *sensitivity assessment.*


Security in the System Life Cycle
Initiation
Development/ Acquisition
Implementation
Operation/ Maintenance
Disposal
Sensitivity Assessment
Determine Security Requirements (including Risk Assessments)
Incorporate Security Requirements into Specifications
Obtain the System (Build/Buy) and Related Security Activities
Install/Turn-On Security Controls
Security Testing (including Certification)
Accreditation
Security Operations and Administration
Operational Assurance (Monitor/Audit)
Managing Change
Periodic Reaccreditation
Computer Security Plan

The life cycle process described in this chapter consists of five separate phases. Security issues are present in each.

Figure 8.1