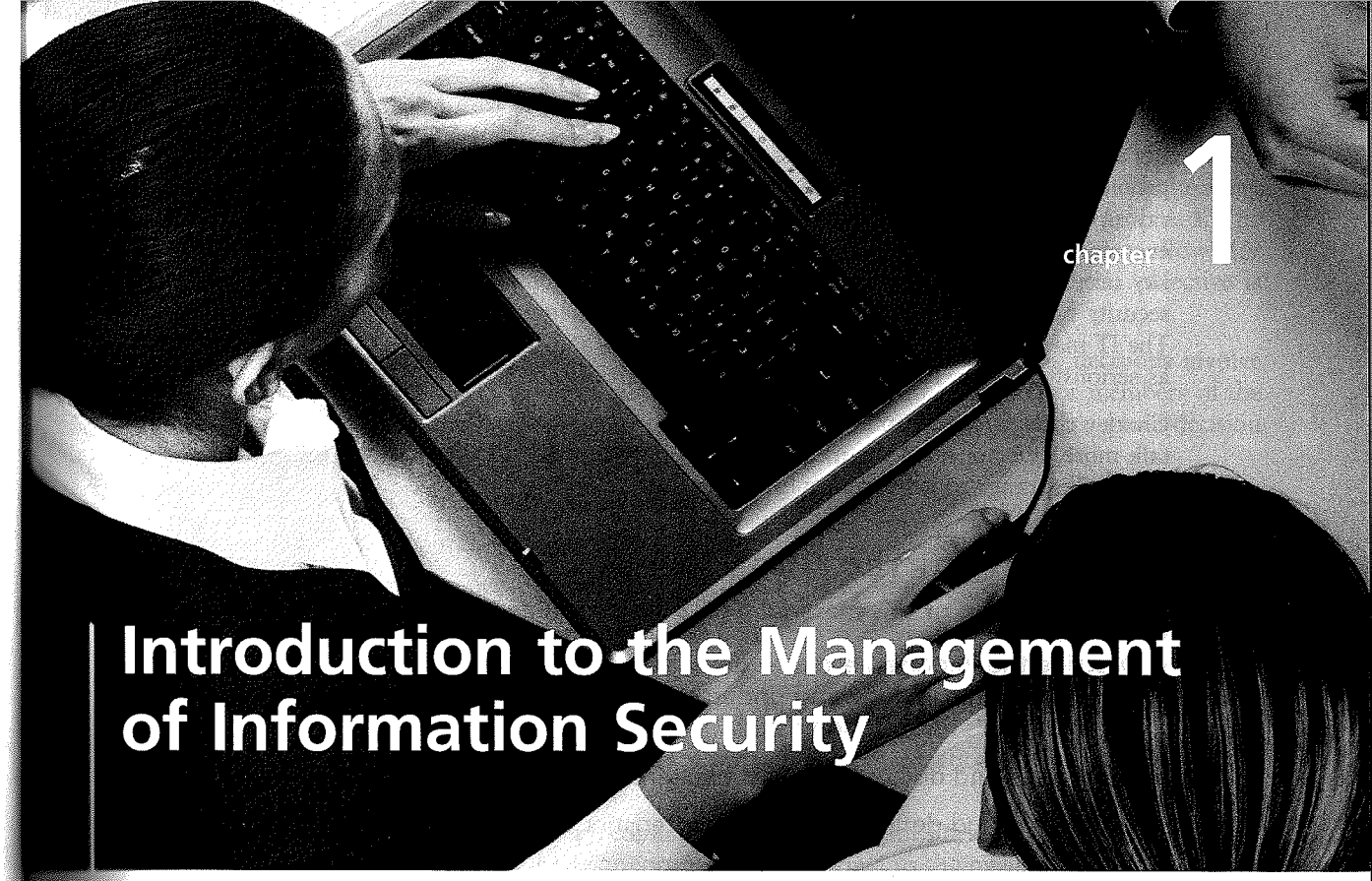


chapter 1

Introduction to the Management of Information Security

If this is the information superhighway, it's going through a lot of bad, bad neighborhoods.

DORIAN BERGER, 1997

One month into her new position at Random Widget Works, Inc. (RWW), Iris Majwabu left her office early one afternoon to attend a meeting of the Information Systems Security Association (ISSA). She had recently been promoted from her previous assignment at RWW as an information security risk manager.

This occasion marked Iris's first ISSA meeting. With a mountain of pressing matters on her cluttered desk, Iris didn't know why she was making it a priority. She sighed. As the first Chief Information Security Officer (CISO) to be named at RWW, she had already spent many hours in business meetings, followed by long hours at her desk working toward defining her new position at the firm.

In the ISSA meeting room she saw Charley Moody, her supervisor from a company she used to work for, Sequential Label and Supply (SLS). Charley had been promoted to Chief Information Officer (CIO) of SLS almost a year ago.

"Hi, Charley," she said.

"Hello, Iris." They shook hands warmly. "Congratulations on your promotion. How are things going in your new position?"

"So far," she replied, "things are going well—I think."

Charley noticed her hesitancy. "You think?" he said. "Okay, tell me what's going on."

Iris explained, "Well, I'm struggling to get a consensus from the management team about the problems we have. I'm told that information security is a priority, but everything is in disarray. Any ideas that are brought up, especially my ideas, are chopped to bits before they're even considered by management. There's no established policy covering our information security needs, and it seems that we have little hope of getting one approved. The information security budget covers my salary plus funding for one technician in the network department. The IT managers act like I'm a waste of their time, and they don't seem to take security issues as seriously as I do. It's like trying to drive a herd of cats!"

Charley thought for a moment and then said, "I've got some ideas that may help. We should talk more, but not now; the meeting is about to start. Here's my number—call me tomorrow and we'll arrange to get together for coffee."

LEARNING OBJECTIVES

Upon completion of this material, you should be able to:

- Describe the importance of the manager's role in securing an organization's use of information technology and understand who is responsible for protecting an organization's information assets
- Enumerate and discuss the key characteristics of information security
- Enumerate and define the key characteristics of leadership and management
- Differentiate information security management from general management
- Identify and implement basic project management practices and techniques

Introduction

In today's global markets, business operations are enabled by technology. From boardroom to mailroom, businesses make deals, ship goods, track client accounts, and inventory company assets, all through the implementation of systems based upon information technology (IT). IT enables the storage and transportation of information—often a company's most valuable resource—from one business unit to another. But what happens if the vehicle breaks down, even for a little while? Business deals fall through, shipments are lost, and company assets become more vulnerable to threats from both inside and outside the firm. In the past, the business manager's response to this possibility was to proclaim, "We have technology people to handle technology problems." This statement might have been valid in the days when technology was confined to the climate-controlled rooms of the data center and when information processing was centralized. In the last 20 years, however, technology has permeated every facet of the business environment. The business place is no longer static—it moves whenever employees travel from office to office, from city to city, or even from office to home. Since businesses have become more fluid, the concept of computer security has evolved into the idea of information security. Because this newer concept covers a broader range of issues, from the protection of data to the protection of human resources, information security is no longer the sole responsibility of a small, dedicated group of professionals in the company. It is now the responsibility of every employee, especially managers.

Astute managers increasingly recognize the critical nature of information security as the vehicle by which the organization's information assets are secured. In response to this growing awareness, businesses are creating new positions to solve the newly perceived problems. The emergence of technical managers, like Iris in the opening scenario of this chapter, allows for the creation of professionally managed information security teams whose main objective is the protection of information assets.

Organizations must realize that information security funding and planning decisions involve more than just technical managers, such as information security managers or members of the information security team. Rather, the process should involve three distinct groups of decision makers, or **communities of interest:**

- Information security managers and professionals
- IT managers and professionals
- Nontechnical general business managers and professionals

These three professional groups should engage in constructive debate to reach consensus on an overall plan to protect the organization's information assets.

The communities of interest fulfill the following roles:

- The **information security community** protects the organization's information assets from the many threats they face.
- The **information technology community** supports the business objectives of the organization by supplying and supporting IT appropriate to the business' needs.
- The nontechnical **general business community** articulates and communicates organizational policy and objectives and allocates resources to the other groups.

Working together, these communities of interest make collective decisions about how to secure an organization's information assets most effectively. As the discussion in this chapter's opening scenario between Iris and Charley suggests, managing a successful information security program takes time, resources, and a lot of effort by all three communities within the organization. Each community of interest must understand that information security is about risk: identifying, measuring, and mitigating—or, at a minimum, documenting—the risk of operating information assets. It is up to the leadership of each of the communities of interest to identify and support initiatives for controlling the risks faced by the organization's information assets. But to make sound business decisions concerning the security of information assets, managers must understand the concept of information security, the roles professionals play within that field, and the issues organizations face in a fluid, global business environment.

What Is Security?

In order to understand the technical aspects of information security, you must know the definitions of certain IT terms and concepts. This knowledge enables you to communicate effectively with the IT and information security communities.

In general, **security** is defined as "the quality or state of being secure—to be free from danger."[1] To be secure is to be protected from adversaries or other hazards. National security, for example, is a system of multilayered processes that protects the sovereignty of a state—its

assets, resources, and people. Achieving an appropriate level of security for an organization also depends on the implementation of a multilayered system. Security is often achieved by means of several strategies undertaken simultaneously or used in combination with one another. Many of the various strategies focus on a specific area of security, but they have many elements in common. It is the role of management to ensure that each strategy is properly planned, organized, staffed, directed, and controlled.

Some the specialized areas of security are:

- **Physical security**, which encompasses strategies to protect people, physical assets, and the workplace from various threats, including fire, unauthorized access, and natural disasters
- **Operations security**, which focuses on securing the organization's ability to carry out its operational activities without interruption or compromise
- **Communications security**, which encompasses the protection of an organization's communications media, technology, and content, and its ability to use these tools to achieve the organization's objectives
- **Network security**, which addresses the protection of an organization's data networking devices, connections, and contents, and the ability to use that network to accomplish the organization's data communication functions

The efforts in each of these areas contribute to the information security program as a whole. This textbook bases its definition of information security on the standards published by the Committee on National Security Systems (CNSS), formerly known as the National Security Telecommunications and Information Systems Security Committee (NSTISSC).

Information security (InfoSec) is the protection of information and its critical characteristics (confidentiality, integrity, and availability), including the systems and hardware that use, store, and transmit that information, through the application of policy, training and awareness programs, and technology. Figure 1-1 shows that information security includes the broad areas of information security management (the topic of this book), computer and data security, and network security; it also shows that policy is the space where these components overlap. (You will learn about policy in detail in Chapter 4).

CNSS Security Model

The CNSS document NSTISSI No. 4011 National Training Standard for Information Security (InfoSec) Professionals (see www.cnss.gov/Assets/pdf/nstissi_4011.pdf) presents one comprehensive model of information security. The CNSS security model, also known as the McCumber Cube after its developer, John McCumber, is rapidly becoming the standard for many aspects of the security of information systems. This model, illustrated in Figure 1-2, shows the three dimensions central to the discussion of information security. If we extend the relationship among the three dimensions represented by the axes shown in the figure, we end up with a 3 × 3 × 3 cube with 27 cells. Each cell represents an area of intersection among these three dimensions that must be addressed to secure information systems. When using this model to design or review any information security program, you must make sure that each of the 27 cells is properly addressed by each of the three communities of interest. For example, the cell representing the intersection between the technology, integrity, and storage areas is expected to include controls or safeguards addressing the use of technology to protect the

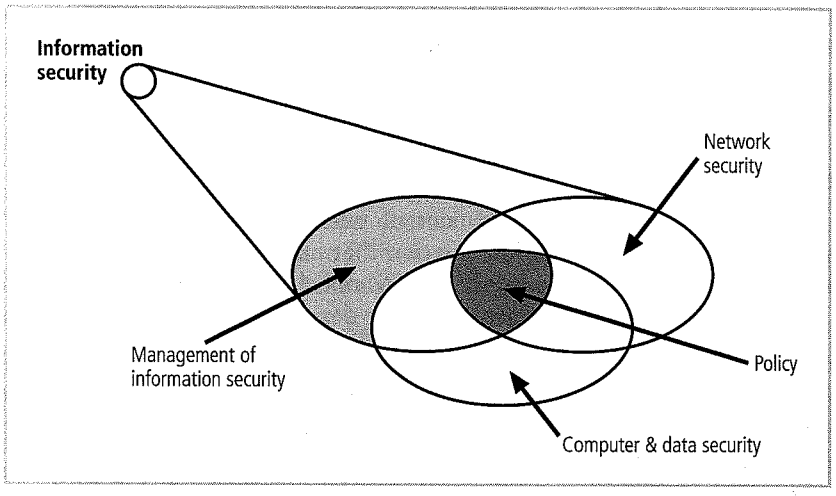


Figure 1-1 Components of information security

Source: Course Technology/Cengage Learning

integrity of information while in storage. Such a control might consist of a host intrusion detection system (HIDS), which alerts the security administrators when a critical file is modified.

While the CNSS model covers the three dimensions of information security, it omits any discussion of the guidelines and policies that direct the implementation of controls, which are essential to an effective information security program. The main purpose of this model is to identify gaps in the coverage of an information security program.

Another weakness of this model emerges when it is viewed from a single perspective. For example, the HIDS control described earlier addresses only the needs and concerns of the information security community, leaving out the needs and concerns of the broader IT and general business communities. In practice, thorough risk reduction requires the creation and dissemination of controls of all three types (policy, education, and technical) by all three

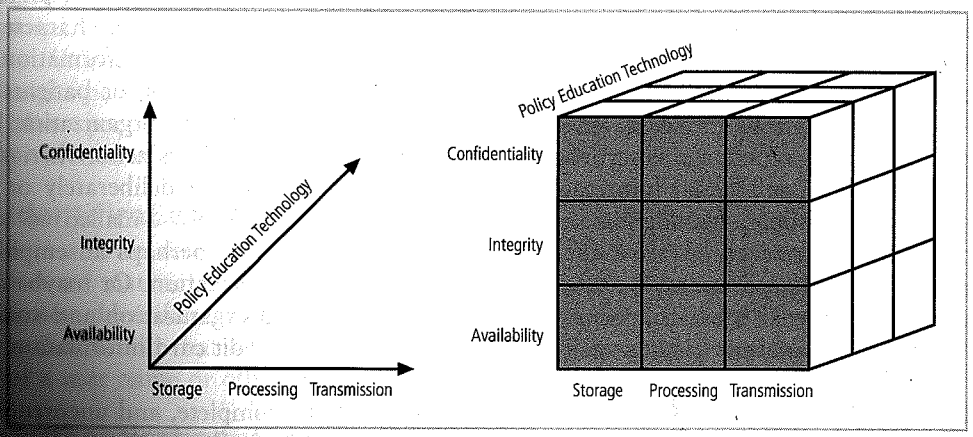


Figure 1-2 CNSS security model

Source: Course Technology/Cengage Learning (adapted from NSTISSI No. 4011)

communities. These controls can be implemented only through a process that includes consensus building and constructive conflict to reflect the balancing act that each organization faces as it designs and executes an information security program. Following chapters of this book will elaborate on these issues.

Key Concepts of Information Security

In order to better understand the management of information security, you must become familiar with the key characteristics of information that make it valuable to an organization. The **C.I.A. triangle**, which is the basis of the CNSS model of information security, has been the industry standard for computer security since the development of the mainframe.

The C.I.A. triangle is founded on three desirable characteristics of information—confidentiality, integrity, and availability—that are as important today as they were when first put forth. However, present-day needs have made these three concepts alone inadequate because they are limited in scope and cannot encompass the constantly changing environment of the IT industry. This new environment of constantly evolving threats has necessitated the development of a more robust model of the characteristics of information. The C.I.A. triangle, therefore, has been expanded into a more comprehensive list of critical characteristics and processes, including privacy, identification, authentication, authorization, and accountability.

Confidentiality **Confidentiality** is the characteristic of information whereby only those with sufficient privileges and a demonstrated need may access certain information. When unauthorized individuals or systems can view information, confidentiality is breached. To protect the confidentiality of information, a number of measures are used, including:

- Information classification
- Secure document storage
- Application of general security policies
- Education of information custodians and end users
- Cryptography (encryption)

Confidentiality is closely related to another key characteristic of information, privacy (discussed later in this chapter). The complex relationship between these two characteristics is examined in detail in Chapter 11. In an organization, confidentiality of information is especially important for personal information about employees, customers, or patients. People expect organizations to closely guard such information. Whether the organization is a federal agency, a commercial enterprise, or a nonprofit charity, problems arise when organizations disclose confidential information. Disclosure can occur either deliberately or by mistake. For example, confidential information could be mistakenly e-mailed to someone outside the organization rather than inside the organization. Or perhaps an employee discards, rather than destroys, a document containing critical information. Or maybe a hacker successfully breaks into an internal database of a Web-based organization and steals sensitive information about clients, such as names, addresses, or credit card information.

Integrity **Integrity** is the quality or state of being whole, complete, and uncorrupted. The integrity of information is threatened when it is exposed to corruption, damage, destruction, or other disruption of its authentic state. Corruption can occur while information is being entered, stored, or transmitted.

Many computer viruses and worms, for example, are designed to corrupt data. For this reason, the key method for detecting an integrity failure of a file system from an attack by a virus or worm is to look for changes in one file's state as indicated by the file's size, or in a more advanced operating system, the file's hash value (discussed later in this section) or checksum (a computed value that remains fixed unless a file has been altered).

The corruption of a file is not always the result of deliberate attacks. Faulty programming or even noise in the transmission channel or media can cause data to lose its integrity. For example, a low-voltage state in a signal carrying a digital bit (a one or zero) can cause the receiving system to record the data incorrectly.

To compensate for internal and external threats to the integrity of information, systems employ a variety of error control techniques, including redundancy bits and check bits. During each transmission, algorithms, hash values, and error-correcting codes ensure the integrity of the information. Data that has not been verified in this manner is retransmitted or otherwise recovered. Because information is of little or no value or use if its integrity cannot be verified, information integrity is a cornerstone of information security.

Availability Availability is the characteristic of information that enables user access to information in a usable format without interference or obstruction. A user in this definition may be either a person or another computer system. Availability does not imply that the information is accessible to any user; rather, it means availability to authorized users.

To understand this concept more fully, consider the contents of a library—in particular, research libraries that require identification for access to the library as a whole or to certain collections. Library patrons must present the required identification before accessing the collection. Once patrons are granted access, they expect to be able to locate and access resources in the appropriate languages and formats.

Privacy Information that is collected, used, and stored by an organization is intended only for the purposes stated by the data owner at the time it was collected. Privacy as a characteristic of information does not signify freedom from observation (the meaning usually associated with the word), but in this context, **privacy** means that information will be used only in ways known to the person providing it. Many organizations collect, swap, and sell personal information as a commodity. It is now possible to collect and combine information on individuals from separate sources, which has yielded detailed databases whose data might be used in ways not agreed to, or even communicated to, the original data owner. Many people have become aware of these practices and are looking to the government for protection of the privacy of their data.

Identification An information system possesses the characteristic of **identification** when it is able to recognize individual users. Identification is the first step in gaining access to secured material, and it serves as the foundation for subsequent authentication and authorization. Identification and authentication are essential to establishing the level of access or authorization that an individual is granted. Identification is typically performed by means of a user name or other ID.

Authentication **Authentication** occurs when a control proves that a user possesses the identity that he or she claims. Examples include the use of cryptographic certificates to establish Secure Sockets Layer (SSL) connections or the use of cryptographic hardware

devices—for example, hardware tokens provided by companies such as RSA's SecurID—to confirm a user's identity.

Authorization After the identity of a user is authenticated, a process called **authorization** assures that the user (whether a person or a computer) has been specifically and explicitly authorized by the proper authority to access, update, or delete the contents of an information asset. An example of authorization is the activation and use of access control lists and authorization groups in a networking environment. Another example is a database authorization scheme to verify that the user of an application is authorized for specific functions such as reading, writing, creating, and deleting.

Accountability **Accountability** of information exists when a control provides assurance that every activity undertaken can be attributed to a named person or automated process. For example, audit logs that track user activity on an information system provide accountability.

What Is Management?

To effectively manage the information security process, you must understand certain core principles of management. In its simplest form, **management** is the process of achieving objectives using a given set of resources. A **manager** is a member of the organization assigned to marshal and administer resources, coordinate the completion of tasks, and handle the many roles necessary to complete the desired objectives. Managers have many roles to play within organizations, including the following:

- **Informational role:** Collecting, processing, and using information that can affect the completion of the objective
- **Interpersonal role:** Interacting with superiors, subordinates, outside stakeholders, and other parties that influence or are influenced by the completion of the task
- **Decisional role:** Selecting from among alternative approaches and resolving conflicts, dilemmas, or challenges

Note that there are differences between leadership and management. A leader influences employees so that they are willing to accomplish objectives. He or she is expected to lead by example and demonstrate personal traits that instill a desire in others to follow. In other words, leadership provides purpose, direction, and motivation to those who follow.

By comparison, a manager administers the resources of the organization. He or she creates budgets, authorizes expenditures, and hires employees. This distinction between a leader and a manager is important, because leadership is not always a managerial function, while nonmanagers are often assigned to leadership roles. Often, however, managers fulfill both the roles of manager and leader.

Behavioral Types of Leaders

There are three basic behavioral types of leaders: the autocratic, the democratic, and the laissez-faire. Autocratic leaders reserve all decision-making responsibility for themselves, and are "do as I say" types of managers. Such a leader typically issues an order to accomplish a task and does not usually seek or accept alternative viewpoints. The democratic leader works in the opposite way, typically seeking input from all interested parties, requesting ideas and suggestions, and then formulating a position that can be supported by a majority.

Each of these two diametrically opposed positions has both strengths and weaknesses. The autocratic leader can be more efficient in that he or she is not constrained by the necessity to accommodate alternative supporting viewpoints. The democratic leader can be less efficient because valuable time is spent in discussion and debate when planning for the task. However, the autocratic leader can be the less effective if that leader's knowledge is less than sufficient for the task. The democratic leader can be more effective when dealing with very complex topics and those in which subordinates have strongly held opinions.

The laissez-faire leader is also known as the "laid-back" leader. While both autocratic and democratic leaders tend to be action-oriented, the laissez-faire leader often sits back and allows the process to develop as it goes, only making minimal decisions to avoid bringing the process to a complete halt.

Effective leaders function with a combination of these styles, shifting approaches as situations warrant. For example, depending on the circumstances, a leader will solicit input when the situation permits, make autocratic decisions when immediate action is required, or allow the operation to proceed if it is progressing in an efficient and effective manner.

Management Characteristics

The management of tasks leading to the accomplishment of any objective requires certain basic skills. These skills are referred to as management characteristics, functions, principles, or responsibilities. The two basic approaches to management are:

- Traditional management theory, which uses the core principles of planning, organizing, staffing, directing, and controlling (POSDC)
- Popular management theory, which categorizes the principles of management into planning, organizing, leading, and controlling (POLC)

The following discussion examines the POLC principles that managers employ when dealing with tasks. Figure 1-3 summarizes these principles and illustrates how they are conceptually related.

Planning The process that develops, creates, and implements strategies for the accomplishment of objectives is called **planning**. Several different approaches to planning are examined more thoroughly in future chapters of this book. The three levels of planning are:

- Strategic planning, which occurs at the highest levels of the organization and for a long period of time, usually five or more years
- Tactical planning, which focuses on production planning and integrates organizational resources at a level below the entire enterprise and for an intermediate duration (such as one to five years)
- Operational planning, which focuses on the day-to-day operations of local resources, and occurs in the present or the short term

Lack of planning can cause the kind of confusion and frustration among managers and staff that Iris describes in the opening scenario of this chapter.

The planning process begins with the creation of strategic plans for the entire organization. The resulting plan is then divided up into planning elements relevant to each major business unit of the organization. These business units in turn create business plans that meet the

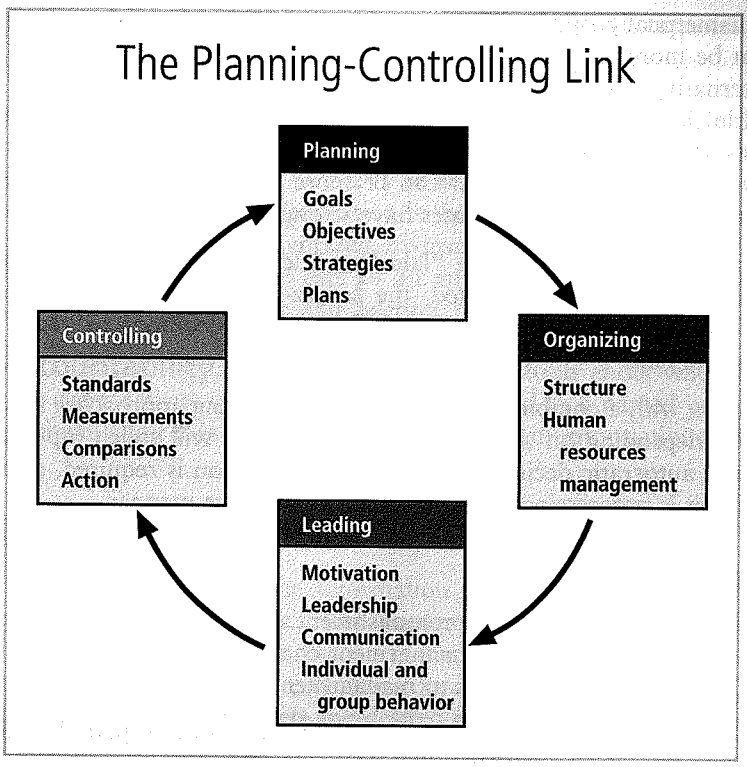


Figure 1-3 The planning-controlling link[2]

Source: Course Technology/Cengage Learning (adapted from Jourdon, 2003)

requirements of the overall organizational strategy. The plans are communicated to midlevel managers so that they can create tactical plans at their levels. Supervisors use the tactical plans to create operational plans that guide the day-to-day operations of the organization. To better understand the planning process, an organization must thoroughly define its goals and objectives. While the exact definition varies depending on context, the term **goal** refers to the end result of a planning process—increasing market share by two percent, perhaps. The term **objective** refers to an intermediate point that allows you to measure progress toward the goal—a growth in sales for each quarter, for example. If you accomplish all objectives in a timely manner, then you are likely to accomplish your goal.

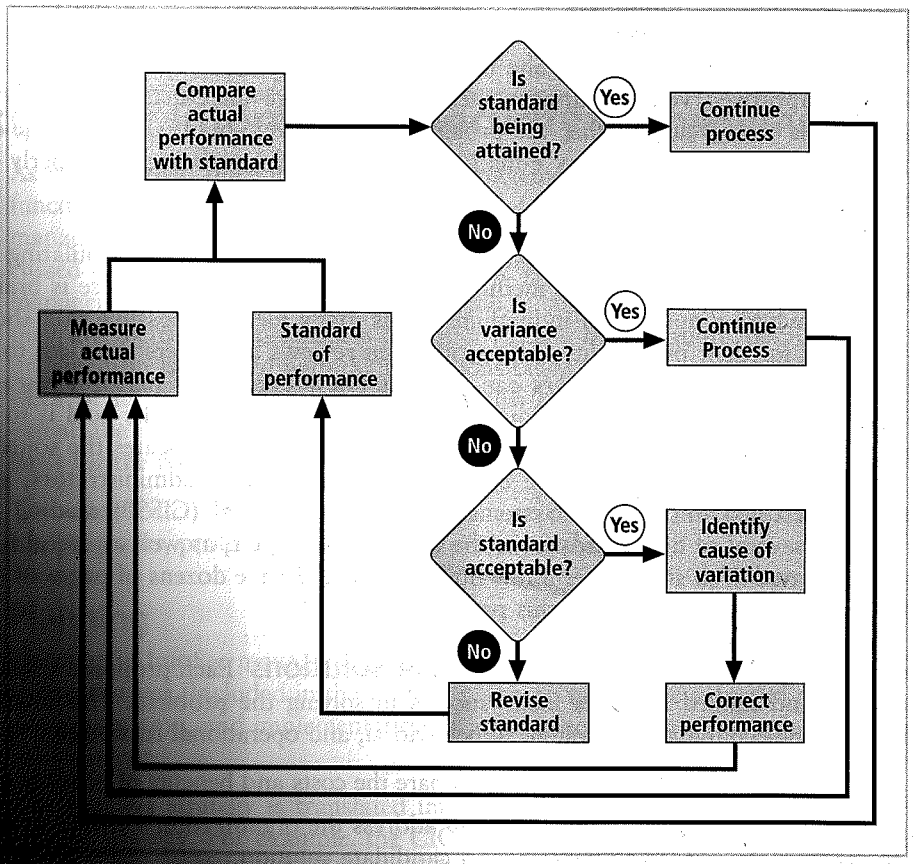
The management of the planning function within an organization encompasses an entire field of study. It requires an understanding of how to plan and a thorough understanding of project management. Project management is discussed in detail later in this chapter.[2]

Organizing The management function dedicated to the structuring of resources to support the accomplishment of objectives is called **organization.** It includes the structuring of departments and their associated staff, the storage of raw materials to facilitate manufacturing, and the collection of information to aid in the accomplishment of the task. Recent definitions of organization include staffing, because organizing people so as to maximize their productivity is not substantially different than organizing time, money, or equipment.

Leading As noted earlier, **leadership** encourages the implementation of the planning and organizing functions. It includes supervising employee behavior, performance, attendance, and attitude. Leadership generally addresses the direction and motivation of the human resource.

Controlling Monitoring progress toward completion, and making necessary adjustments to achieve desired objectives, requires the exercise of **control**. In general, the control function assures the organization of the validity of the plan. The manager ensures that sufficient progress is made, that impediments to the completion of the task are resolved, and that no additional resources are required. Should the plan be found invalid in light of the operational reality of the organization, the manager takes corrective action.

This process relies on the use of cybernetic control loops, often called negative feedback. They all use performance measurements, comparison, and corrective action, as illustrated in Figure 1-4. In this figure, the cybernetic control process begins with a measurement of actual performance, which is then compared to the expected standard of performance as determined by the planning process. If the standard is being met, the process is allowed to continue toward completion. If an acceptable level of performance is not being attained, either the process is corrected to achieve satisfactory results or the expected level of performance is redefined.



The control process

Solving Problems

All managers encounter problems in the course of the organization's day-to-day operation. Whether a problem is low or high profile, the same basic process can be used to solve it. Time pressures often constrain decision making when problems arise, however. The process of gathering and evaluating the necessary facts may be beyond available capabilities. Nevertheless, the methodology described in the following steps can be used as a basic blueprint for resolving many operational problems.

Step 1: Recognize and Define the Problem The most frequent flaw in problem solving is failing to define the problem completely. Begin by clearly identifying exactly which problem needs to be solved. For example, if Iris receives complaints at RWW about the receipt of a large number of unsolicited commercial e-mails (also known as spam), she must first determine whether the complaints are valid. Are employees in fact receiving unsolicited spam, or have they signed up for notifications and mailing lists?

Step 2: Gather Facts and Make Assumptions To understand the background and events that shape the problem, a manager can gather facts about the organizational, cultural, technological, and behavioral factors that are at the root of the issue. He or she can then make assumptions about the methods that are available to solve the problem. For example, by interviewing several employees, Iris might determine that they are receiving a large quantity of unsolicited e-mail. She might also determine that each of these employees has accessed approved vendor support sites, which require an e-mail sign-in process. In such a case, Iris would suspect that the problem of excessive e-mail is, in fact, the result of employees providing their company e-mail addresses, which are being improperly used by the site owners.

Step 3: Develop Possible Solutions The next step is to begin formulating possible solutions. Managers can use several methods to generate ideas. One of these is brainstorming, a process where a number of individuals air as many ideas as possible in a short time, without regard for their practicality. The group then reviews and filters the ideas to identify any feasible options. Problem solvers can also interview experts or perform research into solutions using the Web, magazines, journals, or books. In any case, the goal is to develop as many solutions as possible. In the preceding example, once Iris locates the source of the spam e-mails, she can speak with the e-mail server and firewall administrators, and then turn to her Certified Information Systems Security Professional (CISSP) reading list. She might contact several of her friends from the local ISSA chapter, as well as spend time surfing security-related Web sites. After a few hours, Iris could have dozens of pages of information that might be useful in solving this problem.

Step 4: Analyze and Compare Possible Solutions Each proposed solution must be examined and ranked as to its likely success in solving the problem. This analysis may include reviewing economic, technological, behavioral, and operational feasibilities, as follows:

- To review economic feasibility, you compare the costs and benefits of possible solutions.
- To review technological feasibility, you address the organization's ability to acquire the technology needed to implement a candidate solution.
- To review behavioral feasibility, you assess a candidate solution according to the likelihood that subordinates will adopt and support a solution, rather than resisting it.

- To review operational feasibility, you assess the organization's ability to integrate a candidate solution into its current business processes.

Using this method, you can compare and contrast various proposals. In the spam example, Iris might immediately eliminate any overly expensive solutions, throw out some technical solutions incompatible with RWW's systems, and narrow the field to three alternatives: (1) do nothing, and accept the spam as a cost of doing business, (2) have the e-mail administrator change the users' accounts, or (3) have the firewall administrator filter access to and traffic from the spam sites. Iris could then discuss these alternatives with all administrators involved. Each solution is feasible, inexpensive, and does not negatively affect RWW's overall operations.

Step 5: Select, Implement, and Evaluate a Solution Once a solution is chosen and implemented, you must evaluate it to determine its effectiveness in solving the problem. It is important to monitor the chosen solution carefully so that if it proves ineffective it can be cancelled or altered quickly. In Iris's case, she might decide to implement the firewall filters to reduce the spam, as most of it comes from a few common sources. She might also decide to require the affected employees to attend an e-mail security policy training program, where they can be reminded of the importance of controlling when and where they release company e-mail addresses. In addition, these employees might be required to submit periodic reports regarding the status of the e-mail problem.

Principles of Information Security Management

As noted earlier, information security management is one of the three communities of interest functioning in most organizations. As part of the management team, it operates like all other management units by using the common characteristics of leadership and management discussed earlier in this chapter. However, the goals and objectives of the information security management team differ from those of the IT and general management communities in that they are focused on the secure operation of the organization. Because information security management is charged with taking responsibility for a specialized program, certain characteristics of its management are unique to this community of interest. These unique features extend the basic characteristics of general leadership and management and, as such, form the basis for the balance of this book.

The extended characteristics of information security are known as the six Ps—planning, policy, programs, protection, people, and project management.

Planning

Planning in InfoSec management is an extension of the basic planning model discussed earlier in this chapter. Included in the InfoSec planning model are activities necessary to support the design, creation, and implementation of information security strategies within the IT planning environment.

The business strategy is translated into the IT strategy, which is in turn converted into the information security strategy. For example, the CIO uses the IT objectives gleaned from the business unit plans to create the organization's IT strategy. The IT strategy then informs the planning process for each IT functional area. Depending on the location of the InfoSec function in the organization, the IT strategy may be used for information security planning when the

CISO gets involved with the CIO or other executives to develop the strategy for the next lower level.

The CISO then works with the appropriate security managers to develop operational security plans. These security managers consult with security technicians to develop tactical security plans. Each of these plans is usually coordinated across the IT functions of the enterprise and placed into a master schedule for implementation. The overall goal is to create plans that support long-term achievement of the overall organizational strategy.

If all goes as planned, the entire collection of tactical plans accomplishes the operational goals, and the entire collection of operational goals accomplishes the subordinate strategic goals; this helps to meet the strategic goals and objectives of the organization as a whole.

Several types of InfoSec plans exist, including incident response planning, business continuity planning, disaster recovery planning, policy planning, personnel planning, technology rollout planning, risk management planning, and security program planning including education, training, and awareness. Each of these plans has unique goals and objectives, and each benefits from the same organized, methodical approach. These planning areas are discussed in detail in later chapters of this book.

Another basic planning consideration unique to InfoSec is locating the InfoSec department within the organization structure. This topic is discussed in Chapter 5.

Policy

The set of organizational guidelines that dictates certain behavior within the organization is called **policy**. In InfoSec, there are three general categories of policy:

Enterprise information security policy (EISP) sets the tone for the InfoSec department and the InfoSec climate across the organization. This policy is developed within the context of the strategic IT plan. The CISO typically drafts the program policy, which is usually supported and signed by the CIO or the CEO.

Issue-specific security policies (ISSP) are sets of rules that define acceptable behavior within a specific technology, such as e-mail or Internet usage.

System-specific policies (SysSP) are technical and/or managerial in nature and control the configuration and/or use of a piece of equipment or technology. For example, an access control list (ACL) is a SysSP that defines the accesses permitted for the specified device.

Programs

Programs are the InfoSec operations that are specifically managed as separate entities. A security education training and awareness (SETA) program is one such entity. SETA programs provide critical information to employees to either improve their current level of security knowledge or maintain it. Other programs that may emerge include a physical security program, complete with fire protection, physical access, gates, guards, and so on. Each organization may have one or more security programs that must be managed.

Protection

The protection function is executed via a set of risk management activities, including risk assessment and control, as well as protection mechanisms, technologies, and tools. Each of these mechanisms represents some aspect of the management of specific controls in the overall information security plan.

People

People are the most critical link in the information security program. It is imperative that managers continuously recognize the crucial role that people play in the information security program. This area of InfoSec encompasses security personnel and the security of personnel, as well as aspects of the SETA program mentioned earlier.

Project Management

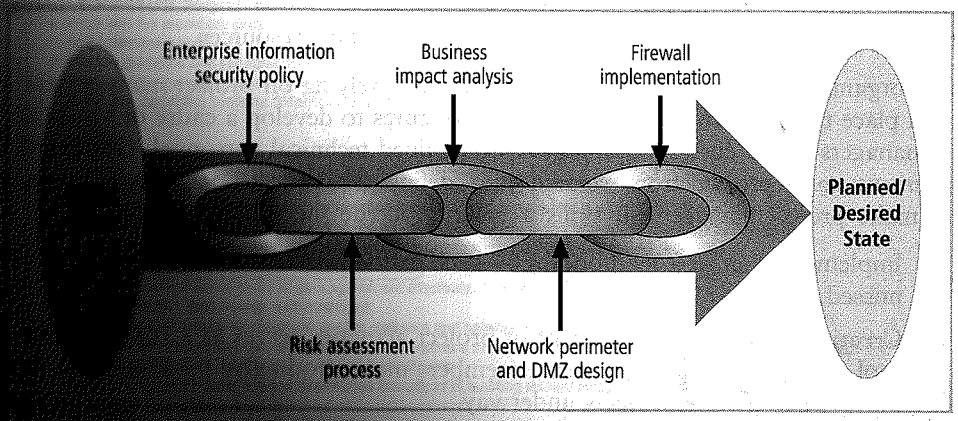
The final component is the application of thorough project management discipline to all elements of the information security program. Whether the task is to roll out a new security training program or to select and implement a new firewall, it is important that the process be managed as a project. Project management involves identifying and controlling the resources applied to the project, as well as measuring progress and adjusting the process as progress is made toward the goal.

Project Management

The need for project management skills within the practice of information security may not at first be self-evident. It is emphasized throughout this book that information security is a process, not a project. However, each element of an information security program must be managed as a project, even if the overall program is perpetually ongoing.

How can information security be both a process and a project? It is, in fact, a continuous series or chain of projects. As illustrated in Figure 1-5, each link in this chain could be a specific project, and each of these projects would be guided by the security systems development life cycle (SecSDLC), described in later chapters.

To be sure, some aspects of information security are not project based; rather, they are managed processes. These managed processes include the monitoring of the external and internal environments during incident response, ongoing risk assessments of routine operations, and continuous vulnerability assessment and vulnerability repair. These activities are called operations, and are ongoing.



security program chain

Course Learning

Projects, on the other hand, are discrete sequences of activities with starting points and defined completion points. In other words, a "project is a temporary endeavor undertaken to create a unique product or service."[3] Although each individual information security project has an end point, larger organizations never completely finish the information security improvement process; they periodically review progress and realign planning to meet business and IT objectives. This realignment can lead to new goals and projects, as well as to the modification, cancellation, or reprioritization of existing projects.

The Guide to the Project Management Body of Knowledge by W. R. Duncan (hereafter called the PMBoK) defines **project management** as:

> *the application of knowledge, skills, tools, and techniques to project activities to meet project requirements. Project management is accomplished through the use of processes such as: initiating, planning, executing, controlling, and closing.*[4]

In other words, project management—which makes use of many of the approaches discussed earlier in this chapter—is focused on achieving the objectives of the project.

Unlike ongoing operations, project management involves the temporary assemblage of a group that completes the project, whose members are then released and perhaps assigned to other projects. Projects are sometimes seen as development opportunities that enable employees and managers to extend their skills in readiness for promotion to larger opportunities. This can lead to one of the common pitfalls in organizations that have operations groups and project teams: the *prima donna* effect, where certain groups are perceived as elite or more skilled than others. This effect is often seen when workers in operations support roles or software maintenance are seen as less dynamic or capable than their project-focused peers.

Although project management is focused on projects that have end points, this does not mean these projects are one-time occurrences. Some projects are iterative and occur regularly. Budgeting processes, for example, are iterative projects. Each year the budget committee meets, designs a proposed budget for the following year, and then presents it to the appropriate manager. The committee may not meet again for six to nine months until the next budget cycle. Another common practice is the creation of a sequence of projects, with periodic submission of grouped deliverables. Each project phase has a defined set of objectives and deliverables, and the authorization to progress to future phases is tied to the success of the preceding phase, as well as to availability of funding or other critical resources.

Some organizational cultures have a long record of relying on project management and have put in place training programs and reward structures to develop a cadre of highly skilled project managers and a corresponding group of trained technical personnel. Other organizations implement each project from scratch and define the process as they go. Organizations that make project management skills a priority accrue the following benefits:

- Implementation of a methodology—such as the SecSDLC—ensures that no steps are missed.
- Creation of a detailed blueprint of project activities serves as a common reference tool, and makes all project team members more productive by shortening the learning curve when getting projects underway.
- Identification of specific responsibilities for all involved personnel lessens ambiguity and reduces confusion when individuals are assigned to new or different projects.

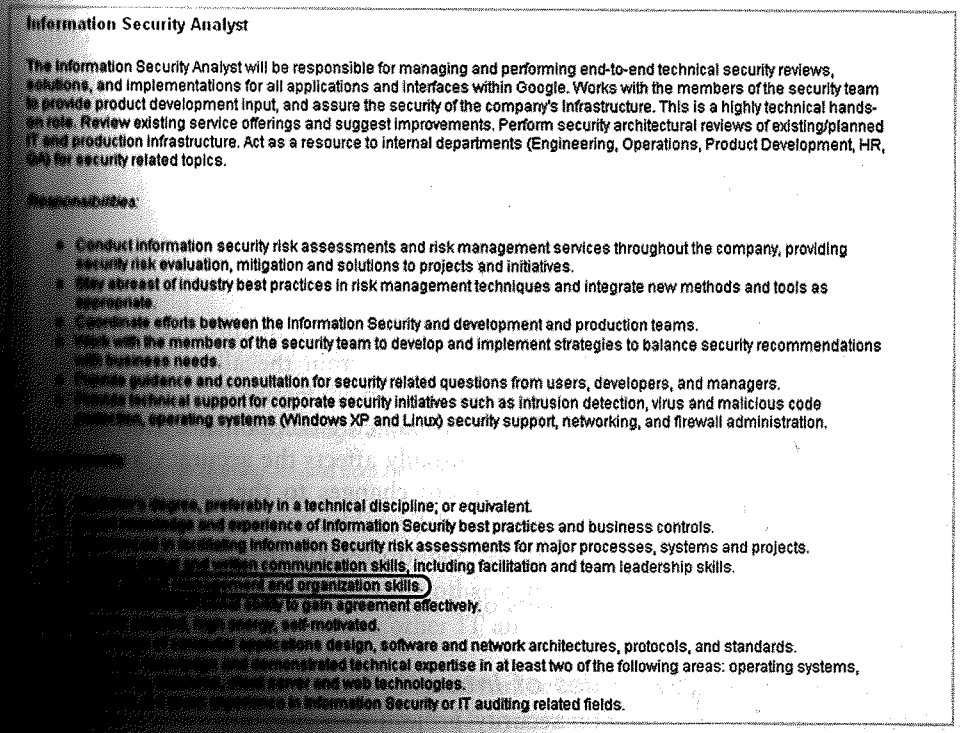
- Clear definition of project constraints, including time frame, budget, and minimum quality requirements increases the likelihood that the project stays within them.
- Establishing measures of performance and creation of project milestones simplifies project monitoring.
- Early identification of deviations in quality, time, or budget enables early correction.

Successful project management relies on careful and realistic project planning coupled with aggressive, proactive control. The project success may be defined differently in each organization, but in general a project is deemed a success when:

- It is completed on time or early.
- It comes in at or below the expenditures planned for in the baseline budget.
- It meets all specifications outlined in the approved project definition, and the deliverables are accepted by the end user and/or assigning entity.

To lead information security projects, some organizations assign technically skilled IT or information security experts; others assign experienced project and general managers. Some organizations use both approaches simultaneously. Regardless of the approach, the goal is the same: to have all elements of the information security program completed with quality deliverables, on a timely basis, and within budget.

The job posting shown in Figure 1-6 shows the typical requirements for an information security analyst.



Information Security Analyst

The Information Security Analyst will be responsible for managing and performing end-to-end technical security reviews, solutions, and implementations for all applications and interfaces within Google. Works with the members of the security team to provide product development input, and assure the security of the company's infrastructure. This is a highly technical hands-on role. Review existing service offerings and suggest improvements. Perform security architectural reviews of existing/planned IT and production infrastructure. Act as a resource to internal departments (Engineering, Operations, Product Development, HR, GA) for security related topics.

Responsibilities

- Conduct information security risk assessments and risk management services throughout the company, providing security risk evaluation, mitigation and solutions to projects and initiatives.
- Stay abreast of industry best practices in risk management techniques and integrate new methods and tools as appropriate.
- Coordinate efforts between the Information Security and development and production teams.
- Work with the members of the security team to develop and implement strategies to balance security recommendations with business needs.
- Provide guidance and consultation for security related questions from users, developers, and managers.
- Provide technical support for corporate security initiatives such as intrusion detection, virus and malicious code protection, operating systems (Windows XP and Linux) security support, networking, and firewall administration.

Qualifications

- [illegible] degree, preferably in a technical discipline; or equivalent.
- [illegible] knowledge and experience of Information Security best practices and business controls.
- [illegible] involved in facilitating Information Security risk assessments for major processes, systems and projects.
- [illegible] and written communication skills, including facilitation and team leadership skills.
- [illegible] project and organization skills.
- [illegible] ability to gain agreement effectively.
- [illegible], high energy, self-motivated.
- [illegible] computer applications design, software and network architectures, protocols, and standards.
- [illegible] and demonstrated technical expertise in at least two of the following areas: operating systems, client server and web technologies.
- [illegible] experience in Information Security or IT auditing related fields.

Sample position posting for an information security analyst

[illegible] Medical Colleges. Reprinted with permission.

Although project management and organizational skills are not included in every information security analyst position description, many employers seek candidates who couple their information security focus and skills with strong project management skills. Many consulting firms now offer information security services in conjunction with, or in the context of, project management.

Applying Project Management to Security

To apply project management to information security, you must first select an established project management methodology. Information security project managers often follow methodologies based on the Project Management Body of Knowledge (PMBoK), a methodology promoted by the Project Management Institute. While other project management approaches exist, the PMBoK is considered the industry best practice. The following sections examine the PMBoK in the context of information security project management.

PMBoK Knowledge Areas

The PMBoK identifies the project management knowledge areas shown in Table 1-1. Each of these areas is discussed in the following sections.

Project Integration Management Project integration management includes the processes required to ensure that effective coordination occurs within and between the project's many components, including personnel. Most projects include a wide variety of elements: people, time, information, financial resources, internal coordination units (other departments), outside coordination units (regulatory agencies, standards organizations), computing resources, and physical resources (meeting rooms), to name a few.

Major elements of the project management effort that require integration include:

- Development of the initial project plan
- Monitoring of progress as the project plan is executed
- Control of the revisions to the project plan as well as control of the changes made to resource allocations as measured performance causes adjustments to the project plan

Project plan development is the process of integrating all of the project elements into a cohesive plan with the goal of completing the project within the allotted work time using no more than the allotted project resources. As shown in Figure 1-7, these three elements—work time, resources, and project deliverables—are core components used in the creation of the project plan. Changing any one element usually affects the accuracy and reliability of the estimates of the other two, and likely requires changes to the project plan. For instance, changing the quality or quantity of project deliverables requires changes in work time or resource allocations in order for the project plan to remain realistic.

When integrating the disparate elements of a complex information security project, complications are likely to arise.

Conflicts Among Communities of Interest When business units do not perceive the need or purpose of an information security project, they may not fully support it. When IT staff are not completely aligned with the objectives of the information security project, or do not fully understand its impact or criticality, they may be less than fully supportive and may

Knowledge area	Focus	Processes
Integration	Elements coordination	Project plan development Project plan execution Overall change control
Scope	Including all necessary work	Initiation Scope planning Scope definition Scope verification
Time	On-time completion	Activity definition Activity sequencing Activity duration estimating Schedule development Schedule control
Cost	Completion within budget	Resource planning Cost estimating Cost budgeting Cost control
Quality	Satisfying target needs	Quality planning Quality assurance Quality control
Human resource	Effectively using workers	Organizational planning Staff acquisition Team development
Communications	Efficiently processing information	Communications planning Information distribution Performance reporting Administrative closure
	Minimizing impact of adverse occurrences	Risk identification Risk quantification Risk response development Risk response control
	Acquiring needed resources	Procurement planning Solicitation planning Solicitation Source selection Contract administration Contract closeout

Project management knowledge areas

Cengage Learning adapted from Project Management Body of Knowledge (PMBoK) by the Project Management Institute

less than a complete effort toward ensuring its success. The information security community must educate and inform the other communities so that information security projects receive the same support as other IT and non-IT projects.

Enterprise-Spanning Impact Many information security projects span the enterprise and may affect every user of an organization's IT systems. Some parts of the organization may not have the same degree of motivation to participate, and in fact, may be opposed to the goals of the project. The project manager may have to build consensus across the organization and

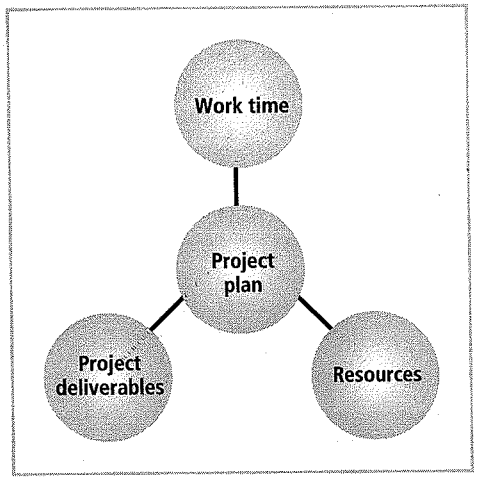


Figure 1-7 Project plan inputs

Source: Course Technology/Cengage Learning

must allow for necessary education, training, and systems integration efforts when estimating work time and resource demands.

Resistance to New Technology Information security projects often introduce new technologies. Depending on an organization's appetite for risk, a project may deploy technology-based controls that are new to the industry as well as to the organization. Sometimes the disparate constituencies that are needed to make a project successful are not open to new or different technologies, and the project manager becomes engaged in debates about technology selections or is required to build consensus around technology choices. Project team members, as well as other workers in the organization, may require special training when new technologies are introduced. This increases the risk of human resource turnover because personnel trained in a new, high-demand skill are more likely to leave the organization for opportunities elsewhere. Proactive steps, such as retention bonuses or gain-sharing arrangements, may help mitigate this risk, but the project plan should include contingency plans for personnel turnover.

Project Scope Management Project scope management includes ensuring that the project plan includes those activities—and only those activities—necessary to complete it. One issue that undermines many projects once they are underway is a phenomenon known as scope creep. **Scope creep** occurs when the quantity or quality of project deliverables is expanded from the original project plan. Stopping scope creep can pose a challenge to many project managers, who seek to meet the objectives expressed to them by project sponsors. Experienced project managers, exposed to project scope creep in the past, are prepared to ask for a corresponding expansion of project work time, project resources, or both.

Major processes of this stage include:

- Scope planning
- Scope definition
- Scope verification

Viewpoint
Okay, Go Ahead and Do It

By Henry Bonin, Consultant, Andromeda Sciences

Congratulations! You've made a commitment to learn about the various components of information security management. When done, you will be able to sew all the pieces together to make comprehensive information security solutions actually happen. A comprehensive solution goes beyond the technology pieces and includes project management, writing supporting plans, developing policies and programs, performing risk assessments, identifying and controlling risks, and hiring the right people to work on the project. These are the skills you will learn in this book.

Imagine: In the near future, you and your team have gone through all the steps of planning and analyzing your concept for some technical element of an information security system, and are presenting a proposal to the decision maker. You convince the boss that this is the right thing to do, and he or she has just given you the go-ahead. Is your response "Yikes!" or "Cool!"?

There is no venture capitalist that invests solely in a technology. When an IT entrepreneur proposes a project, certainly the technology is the first and focal point of the presentation. However, the methods by which this technology will be managed, or steered, to the marketplace is as important to investors as the technology itself. Venture capitalists know that failure to implement critical management elements will be no less detrimental to project success than a failure of the technology itself.

Projects have high failure rates, and the breakdown is usually traceable to failure to follow an accepted methodology or lack of experience in various aspects of management. However, information security projects can fail for a different reason: the incorrect assumption that information security projects are just another IT project. They are not. This book prepares you for those differences and equips you with the skills to manage information security at your organization.

In addition to these three processes, another process is often added by practitioners in the field who wish to retain greater control of the planning process once the project is underway: change control for all requests that would expand project scope.

Project Time Management Project time management entails ensuring that the project is finished by the identified completion date while meeting its objectives. Failure to meet project deadlines is one of the most frequently cited failures in project management. Many completion deadlines are tied to external requirements such as market demands, business alliances, or government regulations. Missing a deadline can sometimes make project completion moot.

Keep in mind that a given result (the deliverable of the project) requires a certain amount of time and resources (money, people, equipment, and so on) to accomplish. Trimming time or

resources from these amounts requires reducing the quantity or quality of the deliverables. Some believe that most of the projects that fail do so in the planning phase, when management underestimates the necessary time and resources, or overestimates the quantity and quality of project deliverables given the available resources.

This management area includes the following processes:

- Activity definition
- Activity sequencing
- Activity duration estimating
- Schedule development
- Schedule control

Project Cost Management Project cost management includes the processes required to ensure that a project is completed within the resource constraints placed on it. Some projects are planned using only a financial budget from which all resources—personnel, equipment, supplies, and so forth—must be procured (see the section "Project Procurement Management" later in this chapter). Other projects have a variety of resources cobbled together with no real financial support, just whatever the managers can scrounge.

This management area includes the following processes:

- Resource planning
- Cost estimating
- Cost budgeting
- Cost control

Project Quality Management Project quality management includes the processes required to ensure that the project adequately meets the project specifications. The common use of the word *quality* may seem vague—what is a quality product to one person may not be to another. In fact, the definition of quality is quite clear. If the project deliverables meet the requirements specified in the project plan, the project has met its quality objective; if they do not, it has not met its quality objectives. Unfortunately, far too often, poorly planned projects do not provide clear descriptions of what the project is to deliver, whether it is a product, a service, or a revised process.

A good plan defines project deliverables in unambiguous terms against which actual results are easily compared. This enables the project team to determine at each step along the way whether all components are being developed to the original specifications. As noted above in the section on scope management, changes made along the way can threaten the overall success of the project. Any change to the definition of project deliverables must be codified, and then the other two areas of project planning—work time and resources—must be reconciled to the changes.

This focus of management includes the following processes:

- Quality planning
- Quality assurance
- Quality control

Project Human Resource Management Project human resource management includes the processes necessary to ensure the personnel assigned to a project are effectively employed. Staffing a project requires careful estimates of the number of worker hours required. Too few people working on a project almost guarantees it will not be completed on time. Too many people working on a project may be an inefficient use of resources and may cause the project to exceed its resource limits.

The management of human resources must address many complicating factors, among them:

- Not all workers operate at the same level of efficiency; in fact, wide variance in the productivity of individuals is the norm. Project managers must accommodate the work style of each project resource while encouraging every worker to be as efficient as possible.
- Not all workers begin the project assignment with the same degree of skill. An astute project manager attempts to evaluate the skill level of some or all of the assigned resources to better match them to the needs of the project plan.
- Skill mixtures among actual project workers seldom match the needs of the project plan. Therefore, in some circumstances workers may be asked to perform tasks for which they are not necessarily well suited, and those tasks take longer and/or cost more than planned.
- Some tasks may require skills that are not available from resources on hand. This might require the project manager to go outside normal channels for a key skill, which almost always results in delays and higher costs.

Managing human resources in information security projects has additional complexities, including:

- Extended clearances may be required. Since some information security projects involve working in sensitive areas of the organization, project managers may have restrictions placed on which resource can be used (for example, only those with the requisite clearances). While this is not yet a common restriction in most commercial organizations, it does affect organizations in the financial sector (banking and brokerage) as well as in many government agencies.
- Often, information security projects deploy technology controls that are new to the organization, and in such cases there is not a pool of skilled resources in that area from which to draw. This can occur in any project that faces a skill shortage, but is more likely in an information security project than in a routine development project.

...jor processes that take place in this management area include:

- ...Organizational planning
- ...Staff acquisition
- ...Team development

...ct **Communications Management** Project communications management ...s the processes necessary to convey the details of activities associated with the project ...involved parties. This includes the creation, distribution, classification, storage, and ...destruction of documents, messages, and other associated project information.

Overcoming resistance to change may be more of a challenge in information security projects than in traditional development projects. In some cases, users and IT partners may be uncertain about the reasons for the project and may be wary of its effect on their work lives. In extreme cases, a project may face hostility from the future users of the system. The only way to counter this resistance is to initiate education, training, and awareness programs. The project manager, usually working in conjunction with the SETA program within the information security department, should communicate the need for the project as early as possible, and should answer any questions about the effect on users of the deployment of the project deliverables.

Major processes associated with this area of project management include:

- Communications planning
- Information distribution
- Performance reporting
- Administrative closure

Project Risk Management Project risk management includes the processes necessary to assess, mitigate, manage, and reduce the impact of adverse occurrences on the project. Project risk management is very similar to normal security risk management, except the scope and scale are usually much smaller because the area to be protected is the individual project and not the entire organization. In many cases, simply identifying and rating the threats facing the project and assessing the probability of the occurrence of these threats is sufficient. The usual purpose of this component is to identify large risks and to plan the mitigation of adverse events should the risks manifest themselves.

Information security projects do face risks that may be different from other types of projects, as noted in the preceding sections. Those projects that face higher-than-normal risks should allow for appropriate planning and perhaps preemptive action to mitigate these risks.

Major processes involved in this area are:

- Risk identification
- Risk quantification
- Risk response development
- Risk response control

Project Procurement Management Project procurement management includes the processes necessary to acquire needed resources to complete the project. Depending on the common practices of the organization, project managers may simply requisition human resources, hardware, software, or supplies from the organization's stocks. Or they may have to specify the required resources, request and evaluate bids, and then negotiatecontracts for them.

Information security projects may have more complex procurement needs than other types of projects because they are more likely than other projects to need different software or hardware products and/or differently skilled human resources than other common types of IT projects.

Major processes involved in this area of project management are:

- Procurement planning
- Solicitation planning

- Solicitation
- Source selection
- Contract administration
- Contract closeout

Project Management Tools

There are many tools that support the management of the diverse resources in complex projects. Some of these tools are modeling approaches, such as PERT or CPM, and others involve the use of software. Most project managers combine software tools that implement one or more of the dominant modeling approaches. A few of the more common models are discussed here. If you are planning to become a project manager, seek out the proper level of training to acquire the needed skills and background to be successful. The most successful project managers gain sufficient skill and experience to earn a certificate in project management.

The Project Management Institute (PMI) is project management's leading global professional association and sponsors two certificate programs:

- The Project Management Professional (PMP): PMP certification is the profession's most globally recognized and respected certification credential. The PMP designation following your name tells current and potential employers that you have a solid foundation of project management knowledge that can be readily applied in the workplace. To be eligible for the PMP certification, you must first meet specific education and experience requirements and agree to adhere to a code of professional conduct. The final step in becoming a PMP is passing a multiple-choice examination designed to objectively assess and measure your project management knowledge.
- Certified Associate in Project Management (CAPM): The CAPM is a logical stepping-stone to the PMP and a boon to your overall professional development. The CAPM is intended for those practitioners who provide project management services but are relatively new to the profession. Like the PMP, CAPM candidates must first meet specific education and experience requirements and then pass an examination.

Most project managers engaged in the execution of project plans that are nontrivial in scope use tools to facilitate scheduling and execution of the project. A project manager usually determines that certain tasks cannot be performed until prerequisite tasks are complete. It is almost always advantageous to determine in what order tasks must be performed. It is equally important to determine what tasks must not be delayed to avoid holding up the entire project.

Overly complex project management tools often results in a complication called projectitis—a common pitfall of IT and information security projects. **Projectitis** occurs when the project team spends more time documenting project tasks, collecting performance measurements, updating project task information, and updating project completion forecasts than accomplishing meaningful project work. The development of an overly elegant, microscopically detailed plan before gaining consensus for the work and related coordinated activities that it represents is a precursor to projectitis. However, the proper use of project tools can help project managers organize and coordinate project activities and can enhance communication among project team.

The following sections discuss some of the more commonly used project management tools.

Work Breakdown Structure

A project plan can be created using a very simple planning tool, such as the **work breakdown structure (WBS)** shown in Table 1-2. The WBS can be prepared with a simple desktop PC spreadsheet program, as well as with more complex project management software tools.

In the WBS approach, the project plan is first broken down into a few major tasks. Each of these major tasks is placed on the WBS task list. The minimum attributes that should be identified for each task are:

- The work to be accomplished (activities and deliverables)
- Estimated amount of effort required for completion, in hours or workdays
- The common or specialty skills needed to perform the task
- Task interdependencies

As the project plan develops, additional attributes can be added, including:

- Estimated capital expenses for the task
- Estimated noncapital expenses for the task
- Task assignment according to specific skills
- Start and end dates, once tasks have been sequenced and dates projected

Each major task on the WBS is then further divided into either smaller tasks or specific action steps. For simplicity, the sample WBS later in this chapter divides each task only into action steps. In an actual project plan, tasks are often more complex; you may need to subdivide major tasks before action steps can be determined and assigned. Although there are few hard-and-fast rules as to the appropriate level of detail, generally a task or subtask becomes an action step when it can be completed by one individual or skill set, and when it results in a single deliverable.

Task	Effort (hours)	Skill	Dependencies
1. Contact field office and confirm network assumptions	2	Network architect	
2. Purchase standard firewall hardware	4	Network architect and purchasing group	1
3. Configure firewall	8	Network architect	2
4. Package and ship firewall to field office	2	Intern	3
5. Work with local technical resource to install and test firewall	6	Network architect	4
6. Complete network vulnerability assessment	12	Network architect and penetration test team	5
7. Get remote office sign-off and update all network drawings and documentation	8	Network architect	6

Table 1-2 Early draft work breakdown structure

Source: Course Technology/Cengage Learning

Work To Be Accomplished The first step in the WBS is to identify the work to be accomplished in the task or task area; that is, the activities and deliverables. A deliverable is a completed document or program module that is either the beginning point for a later task or an element of the finished project. Ideally, the project planner provides a label for the task followed by a thorough description. The description should be complete enough to avoid ambiguity during the later tracking process, but not so detailed as to make the WBS unwieldy. For instance, if the task is to write firewall specifications for the preparation of a request for proposal (RFP), the planner would note that the deliverable is a specification document suitable for distribution to vendors.

Amount of Effort Planners need to estimate the effort required to complete each task, subtask, or action step. Estimating effort hours for technical work is a complex process. Even when an organization has formal governance, technical review processes, and change control procedures, it is always good practice to ask the individuals who are most familiar with the work or with similar types of work to make the estimates. Then, those assigned to action steps should review the estimated effort hours, understand the tasks, and agree with the estimates.

Skill Sets/Human Resources The project planner should describe the skill set or person (often called a human resource) needed to accomplish the task. Naming individuals should be avoided in the early planning efforts. Instead, the plan should focus on roles or known skill sets. For example, if any of the engineers in the networks group can write the specifications for a router, the assigned resource is "network engineer" on the WBS. As planning progresses to a more detailed level, however, the specific tasks and action steps should be assigned to specific people. For example, when only the manager of the networks group can evaluate the responses to the RFP and make an award for a contract, the planner identifies the network manager by name as the resource.

Task Dependencies Planners should note wherever possible when a task or action step is dependent on other tasks or actions steps. Tasks or action steps that come before a particular task are called predecessors; tasks or action steps that come after a particular task are called successors. There is more than one type of dependency; most courses on project management cover this subject in detail.

Estimated Capital Expenses Planners need to estimate the expected capital expenses for the completion of each task, subtask, or action item. While each organization budgets and expends capital according to its own established procedures, most differentiate between expenses for durable assets and expenses for other purposes. Be sure to determine the practices in place at the organization where the plan is to be used. For example, a firewall device costing $5000 may be a capital expense for a given organization, but the same organization may not consider a $5000 software package to be a capital expense.

Estimated Noncapital Expenses Planners need to estimate the expected noncapital expenses for the completion of each task, subtask, or action item. Some organizations include this cost include a recovery charge for staff time, while others exclude employee time and only contract or consulting time as a noncapital expense. Organizations follow established procedures in classifying different kinds of expenses as being capital or noncapital. As mentioned earlier, it is important to determine the practices in place at the organization where the plan is to be used. For example, an information security

management program costing $600,000 may be considered a noncapital expense, but a network router that costs $600 may be considered a capital expense.

Start and End Dates In the early stages of planning, the project planner should focus on determining completion dates only for major milestones within the project. A milestone is a specific task completion point in the project plan that has a notable effect on the progress of the project plan as a whole. For example, the date for sending the final RFP to vendors is considered a milestone, because it signals that all RFP preparation work is complete. Early in the planning process, assigning too many dates to too many tasks can be a symptom of projectitis. By assigning only key or milestone start and end dates early in the process, planners can avoid this pitfall. Later in the planning process, additional start and end dates can be added as needed.

The following sample project plan can help you better understand the process of creating one. The project is to design and implement a firewall for a single small office. The hardware is a standard organizational product and will be installed at a location that already has a network connection. The first step toward creating the early draft WBS shown in Table 1-2 is to list the major tasks:

- Contact field office and confirm network assumptions.
- Purchase standard firewall hardware.
- Configure firewall.
- Package and ship firewall to field office.
- Work with local technical resource to install and test it.
- Complete vulnerability assessment by the penetration test team.
- Get remote office sign-off and update all network drawings and documentation.

After the project manager has compiled the draft WBS and consulted with specific participants of the project team, additional detail is added and more dates are assigned to tasks. Another, more detailed version emerges, as shown in Table 1-3. The project plan has been further developed and illustrates the breakdown of tasks 2 and 6 into action steps.

Once the project manager has completed the WBS by breaking tasks into subtasks, estimating effort, and forecasting the necessary resources, the work phase—during which the project deliverables are prepared—may begin. A more complex project may require the use of more complex models to complete the task-sequencing effort.

Task-Sequencing Approaches

Sequencing tasks and subtasks in a large and complex project can be truly daunting. Once a project reaches even a relatively modest size, say a few dozen tasks, there can be almost innumerable possibilities for task assignment and scheduling. Fortunately, a number of approaches are available to assist the project manager in this sequencing effort.

Network Scheduling One method for sequencing tasks and subtasks in a project plan is known as network scheduling. The word *network* in this context does not refer in any way to computer networks; rather, it refers to the web of possible pathways to project completion from the beginning task to the ending task. For example, activity A must occur before activity B, which in turn must occur before activity C; a network diagram illustrating this network dependency is shown in Figure 1-8.

Task	Effort (hours)	Skill	Dependencies	Capital expenses	Noncapital expenses	Start and end dates
1. Contact field office and confirm network assumptions; notify penetration test team of intent for test	2	Network architect		0	200	S:9/22 E:9/22
2. Purchase standard firewall hardware						
2.1 Order firewall through purchasing group	1	Network architect	1	4500	100	S:9/23 E:9/23
2.2 Order firewall from group manufacturer	2	Purchasing group	2.1		100	S:9/24 E:9/24
2.3 Firewall delivered	1	Purchasing group	2.2		50	E:10/3
Configure	8	Network architect	2.3		800	S:10/3 E:10/5
Package and ship to field	2	Intern	3		85	S:10/6 E:10/15
with local resource and test	6	Network architect	4		600	S:10/22 E:10/31
tion test						
test	1	Network architect	5		100	S:11/1 E:11/1
test	9	Penetration test team	6.1		900	S:11/2 E:11/12
of	2	Network architect	6.2		200	S:11/13 E:11/15
	8	Network architect	6.3		800	S:11/16 E:11/30

draft work breakdown structure

Cengage Learning

illustration is very simple, the method of depiction gains value as the number of subtasks increases and information is added about the effort and type of resources complete each activity. If multiple activities can be completed concurrently, this in the diagram. If a single activity has two or more prerequisites, or is the com- for two or more activities, this can also be depicted, as shown in Figure 1-9.

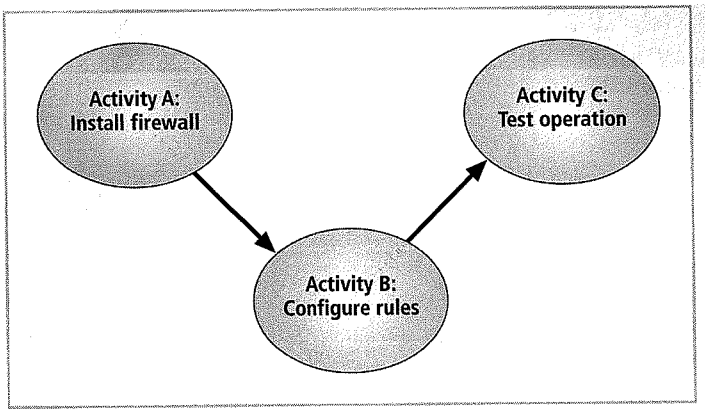


Figure 1-8 Simple network dependency

Source: Course Technology/Cengage Learning

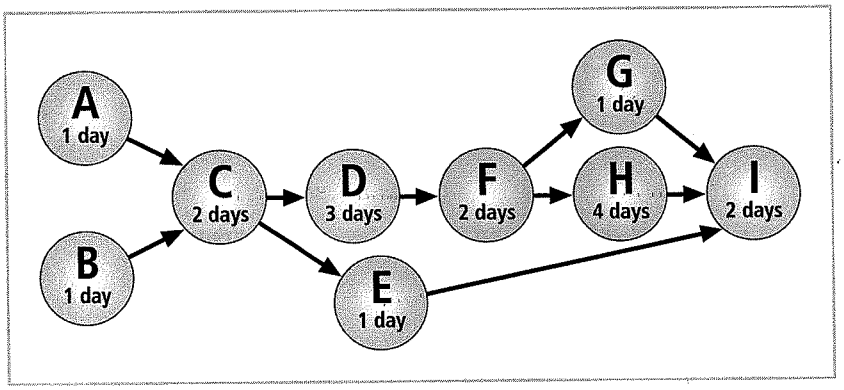


Figure 1-9 Complex network dependency

Source: Course Technology/Cengage Learning

The most popular of networking dependency diagramming techniques is the **Program Evaluation and Review Technique (PERT)**. PERT was originally developed in the late 1950s to meet the needs of the rapidly expanding engineering projects associated with government acquisitions such as weapons systems. About the same time, a similar technique, called the **Critical Path Method (CPM)**, was being developed in the industry. The PERT diagram, as illustrated in Figure 1-10, shows a number of events followed by key activities and their duration. It is possible to take a very complex operation and diagram it in PERT if you can answer three key questions about each activity:

- How long will this activity take?
- What activity occurs immediately before this activity can take place?
- What activity occurs immediately after this activity?

By identifying the path through the various activities, you can determine the critical path. The **critical path** is the sequence of events or activities that requires the longest duration to complete, and that therefore cannot be delayed without delaying the entire project. The difference

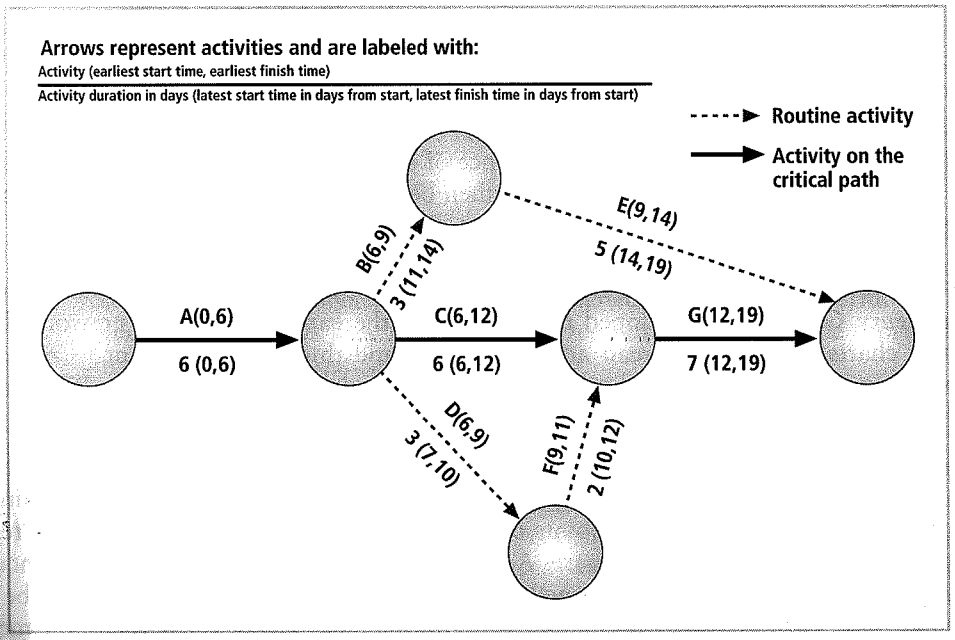


Figure 1-10 PERT example

Source: Course Technology/Cengage Learning

in time between the critical path and any other path is called **slack time**. All tasks not on the critical path have slack time, and thus can be delayed or postponed, within the limits of their slack time, without delaying the entire project. In Figure 1-10, the critical path is the sequence of events ACG, shown by the heavier arrows. A project can have more than one critical path, if two or more paths have the same total time requirement. In the example shown in Figure 1-10, the noncritical path ADFG has one day of slack time. This path can incur a delay of up to one day without adversely affecting the overall completion of the project.

Among the advantages to the PERT method are:

- Planning large projects is made easier by facilitating the identification of pre- and post activities.
- Planning to determine the probability of meeting requirements (that is, timely delivery through calculation of critical paths) is allowed.
- The impact of changes on the system are anticipated. Should a delay in one area occur, how does it affect the overall project schedule?
- Information is presented in a straightforward format that both technical and nontechnical managers can understand and refer to in planning discussions.
- No formal training is required. After a brief explanation most people understand it thoroughly.

Disadvantages of the PERT method include:

- Diagrams can become awkward and cumbersome, especially in very large projects.
- Diagrams can become expensive to develop and maintain due to the complexities of large project development processes.

- It can be difficult to place an accurate "time to complete" on some tasks, especially in the initial construction of a project; inaccurate estimates invalidate any close critical path calculations.

The Critical Path Method is similar in design to the PERT method. CPM relies on a scheduling process designed to identify the sequence of tasks that make up the shortest elapsed time to complete the project. Other tasks may then be scheduled in ways that do not lengthen the total time of the project. In most other ways, CPM is very similar to PERT.

Gantt Chart Another popular project management tool is the bar or Gantt chart, named for Henry Gantt, who developed this method in the early 1900s. Like network diagrams, Gantt charts are simple to read and understand and thus easy to present to management. These simple bar charts are even easier to design and implement than the PERT diagrams and yield much of the same information.

The Gantt chart lists activities on the vertical axis of a bar chart and provides a simple time line on the horizontal axis. A bar represents each activity, with its starting and ending points coinciding with the appropriate points on the time line. The length of the bar thus represents the duration of that particular phase. Activities that overlap can be performed concurrently. Those that do not must be performed sequentially. A vertical reference line can be used to evaluate the current date. Some implementations of the Gantt chart use a fill method to show percentage completion of particular activities. As shown in Figure 1-11, the Gantt chart can provide a wealth of information in a simple format. Activity A has been completed; activity B is ahead of schedule; activity C is behind schedule. Milestones can be added to individual activities, and are usually represented by a numbered triangle just above the bar. These milestones might include the completion of a key report or a component that requires outside interventions. Whatever the case, this method of tracking has proven so simple to use, yet so effective, that it is frequently the preferred method of tracking project progress.

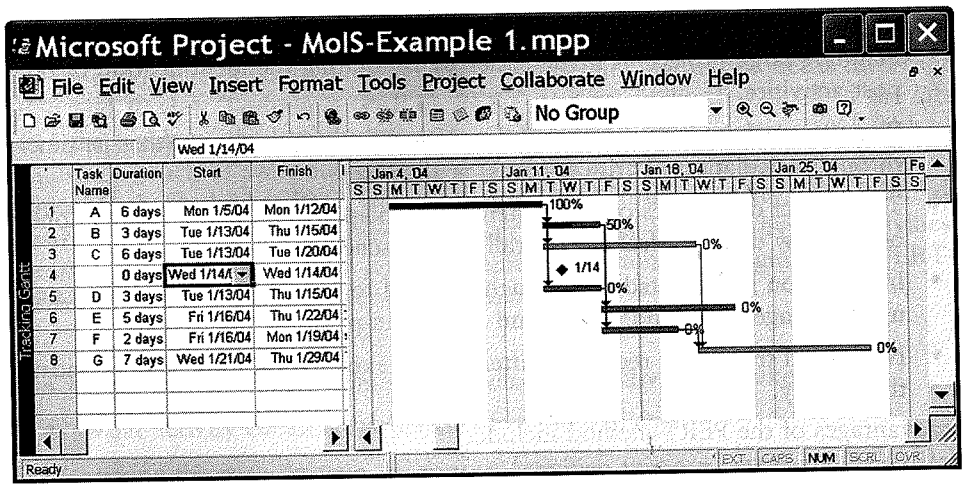


Figure 1-11 Project Gantt chart

Source: Course Technology/Cengage Learning

Automated Project Tools

Microsoft Project is a commonly used project management tool. While it is not the only automated project management tool (there are quite few), and is not universally perceived as the best (that is a matter of heated opinion among project managers), it is generally acknowledged to be the most widely used. If you are considering using an automated project management tool, keep the following in mind:

- A software program cannot take the place of a skilled and experienced project manager who understands how to define tasks, allocate scarce resources, and manage the resources that are assigned. While an automated tool can be powerful in the hands of someone who knows how to use it, it can temporarily disguise the shortcomings of an unprepared project manager.
- A software tool can get in the way of the work. A project manager who spends more than a small amount of time using a tool to record progress and forecast options is on the way to projectitis. Sufferers of this condition spend many hours tweaking project details and calculating trade-offs without making any measurable progress toward completing the project. When project workers must use unfamiliar procedures to report progress in minute detail, they may become less productive. When status meetings turn into lengthy slideshows detailing each aspect of progress, experienced project managers will wonder why team members not working on their assigned tasks.
- Choose a tool that you can use effectively. Any project manager is better served using a tool they know than an overly complex tool they cannot use to good effect. Multimillion-dollar projects have been brought in on time and under budget using nothing more than a simple spreadsheet and lots of hard work. On the other hand, a project manager using state-of-the-art tools can trim weeks from a schedule and save thousands of dollars while meeting every deliverable requirement.

Chapter Summary

- Because businesses and technology have become more fluid, the concept of computer security has been replaced by the concept of information security.
- From an information security perspective, organizations often have three communities of interest: information security managers and professionals, IT managers and professionals, and nontechnical managers and professionals.
- The C.I.A. triangle is based on three desirable characteristics of information: confidentiality, integrity, and availability.
- In its simplest form, management is the process of achieving objectives by using resources.
- The important distinction between a leader and a manager is that a leader influences employees so that they are willing to accomplish objectives, whereas a manager creates budgets, authorizes expenditures, and hires employees.
- The traditional approach to management theory uses the core principles of planning, organizing, staffing, directing, and controlling (POSDC). Another approach to management theory categorizes the principles of management into planning, organizing, leading, and controlling (POLC).

- The process that develops, creates, and implements strategies for the accomplishment of objectives is called planning. There are three levels of planning: strategic, tactical, and operational.
- Information security management operates like all other management units, but the goals and objectives of the InfoSec management team are different in that they focus on the secure operation of the organization.
- Project management is the application of knowledge, skills, tools, and techniques to project activities to meet project requirements. Project management is accomplished through the use of processes that include initiation, planning, execution, controlling, and closing.
- The creation of a project plan can be accomplished using a very simple planning tool, such as the work breakdown structure (WBS).
- A set of methods that can be used to sequence the tasks and subtasks in a project plan is known as network scheduling. Popular techniques include the Program Evaluation and Review Technique (PERT), the Critical Path Method, and the Gantt chart.
- Automated project management tools can assist experienced project managers in the complexities of managing a large project, but may get in the way when used by novice project managers or when used on simple projects.

Review Questions

1. List and describe an organization's three communities of interest that engage in efforts to solve InfoSec problems. Give two or three examples of who might be in each community.
2. What is the definition of information security? What essential protections must be in place to protect information systems from danger?
3. What is the C.I.A. triangle? Define each of its component parts.
4. Describe the CNSS security model. What are its three dimensions?
5. What is the definition of *privacy* as it relates to information security? How is this definition of *privacy* different from the everyday definition? Why is this difference significant?
6. Define the InfoSec processes of identification, authentication, authorization, and accountability.
7. What is management and what is a manager? What roles do managers play as they execute their responsibilities?
8. How are leadership and management similar? How are they different?
9. What are the characteristics of management based on the popular approach to management? Define each characteristic.
10. What are the three types of general planning? Define each.
11. List and describe the five steps of the general problem-solving process.
12. Define *project management*. Why is project management of particular interest in the field of information security?

13. Why are project management skills important to the information security professional?
14. How can security be both a project and a process?
15. What are the nine areas that make up the component processes of project management?
16. What are the three planning parameters that can be adjusted when a project is not being executed according to plan?
17. Name and briefly describe some of the manual and automated tools that can be used to help manage projects.
18. What is a work breakdown structure and why is it important?
19. List and describe the various approaches to task sequencing.
20. How do PERT/CPM methods help to manage a project?

Exercises

1. Assume that a security model is needed for the protection of information in your class. Using the CNSS model, examine each of the cells and write a brief statement on how you would address the components represented in that cell.
2. Consider the information stored in your personal computer. Do you, at this moment, have information stored in your computer that is critical to your personal life? If that information became compromised or lost, what effect would it have on you?
3. Draft a work breakdown structure for the task of implementing and using a PC-based virus detection program (one that is not centrally managed).
4. Your instructor has been provided with an Instructor Resources Kit that includes several MS Project files. If you have access to MS Project and can access the file MoIS_12_01.mpp, you can perform this exercise.

   Open the project file. Make a note of the project completion date as shown in the Gantt chart. (You can easily see this date by clicking **Project | Project Information** in the menu bar.) Now, change the predecessors in task G from 3, 7 to 3, 6. Check the completion date again. What happened? Why?
5. Your instructor has been provided with an Instructor Resources Kit that includes several MS Project files. If you have access to MS Project and can access the file MoIS_12_02.mpp, you can perform this exercise.

   Open the project file. When is the project scheduled to begin? When will it be completed? Which phase will take the longest to complete?

[illegible]

[illegible] made an appointment to meet for a working lunch the next week. Charley [illegible] day before the meeting to jot down his thoughts about good advice for Iris.

[illegible] good to do, Iris," Charley said, "is to find someone skilled in project manage- [illegible] someone off to PM training."

"Why so?" Iris asked.

"A good project manager can help the entire team learn how to manage all the security projects to keep you from getting overwhelmed with deadlines and deliverables." Charley smiled. "A good PM can make your operations proactive rather than reactive."

"That sounds good," Iris replied. "What else do I need to know?"

a. Based on your reading of the chapter and what you now know about the issues, list at least three other things Charley could recommend to Iris.

b. From Charley's advice to Iris, what do you think is the most important? Why?

Endnotes

1. Merriam-Webster. "security." Merriam-Webster Online. [Cited 1 February 2002]. Available from the World Wide Web at www.m-w.com/cgi-bin/dictionary.
2. From the lecture notes of Dr. Louis Jourdan, Clayton College and State University. [Cited April 15, 2003]. Available from the World Wide Web at http://business.clayton.edu/ljourdan/mgmt3101ic/.
3. W. R. Duncan. A Guide to the Project Management Body of Knowledge. 1996, Project Management Institute, 3.
4. W. R. Duncan. A Guide to the Project Management Body of Knowledge. 1996, Project Management Institute, 6.