UNIT 1

INTRODUCTION TO CYBERSECURITY

Introduction –

1.1. Introduction:

Cyber Security is a process that's designed to protect networks and devices from external threats. Businesses typically employ Cyber Security professionals to protect their confidential information, maintain employee productivity, and enhance customer confidence in products and services.

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

The History of Information Security

The history of information security begins with **computer security**. The need for computer security—that is, the need to secure physical locations, hardware, and software from threats—arose during World War II when the first mainframes, developed to aid computations for communication code breaking were put to use. Multiple levels of security were implemented to protect these mainframes and maintain the integrity of their data. Access to sensitive military locations, for example, was controlled by means of badges, keys, and the facial recognition of authorized personnel by security guards. The growing need to maintain national security eventually led to more complex and more technologically sophisticated computer security safe guards.

What Is Security?

In general, **security** is "the quality or state of being secure—to be free from danger."11 In other words, protection against adversaries—from those who would do harm, intentionally or otherwise—is the objective. National security, for example, is a multilayered system that protects the sovereignty of a state, its assets, its resources, and its people. Achieving the appropriate level of security for an organization also requires a multifaceted system.

A successful organization should have the following multiple layers of security in place to protectits operations:

Physical security, to protect physical items, objects, or areas from unauthorized access

and misuse

Personnel security, to protect the individual or group of individuals who are authorized to access the organization and its operations

Operations security, to protect the details of a particular operation or series of activities

Communications security, to protect communications media, technology, and content

Network security, to protect networking components, connections, and contents

Information security, to protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission. It is achieved via the application of policy, education, training and awareness, and technology.

The Committee on National Security Systems (CNSS) defines information security as the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information.12 Figure 1-3 shows that information security includes the broad areas of information security management, computer and data security, and network security. The CNSS model of information security evolved from a concept developed by the computer security industry called the C.I.A. triangle. The C.I.A. triangle has been the industry standard for computer security since the development of the mainframe. It is based on the three characteristics of information that give it value to organizations: confidentiality, integrity, and availability. The security of these three characteristics of information is as important today as it has always been, but the C.I.A. triangle model no longer adequately addresses the constantly changing environment. The threats to the confidentiality, integrity, and availability of information have evolved into a vast collection of events, including accidental or intentional damage, destruction, theft, unintended or unauthorized modification, or other misuse from human or nonhuman threats. This new environment of many constantly evolving threats has prompted the development of a more robust model that addresses the complexities of the current information security environment. The expanded model consists of a list of critical characteristics of information, which are described in the next section. C.I.A. triangle terminology is used in this chapter because of the breadth of material that is based on it.

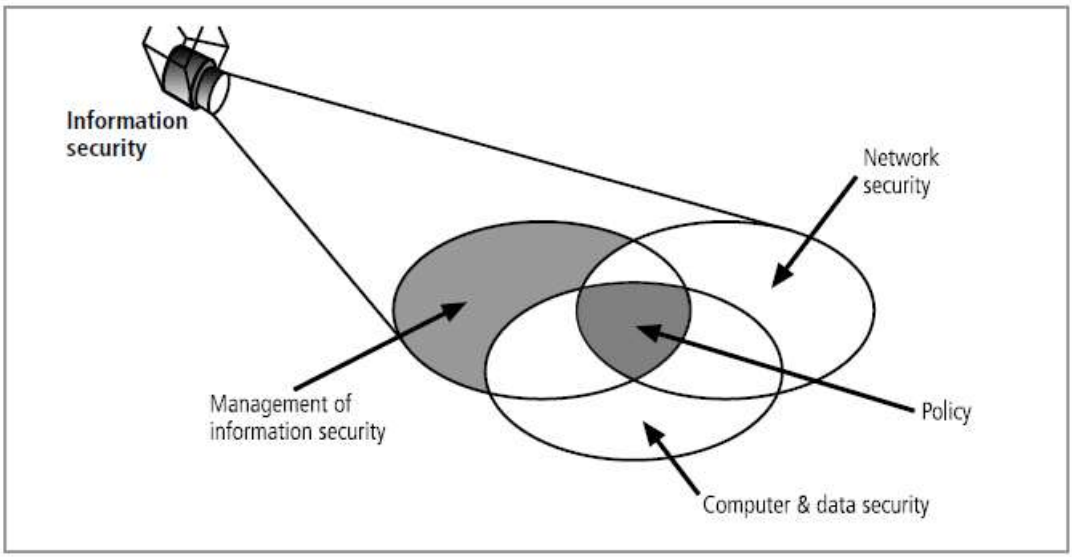


Figure 1-3 Components of Information Security

Source: Course Technology/Cengage Learning

Key Information Security Concepts

Access: A subject or object's ability to use, manipulate, modify, or affect another subject or object. Authorized users have legal access to a system, whereas hackers have illegal access to a system. Access controls regulate this ability.

Asset: The organizational resource that is being protected. An asset can be logical, such as a Web site, information, or data; or an asset can be physical, such as a person, computer system, or other tangible object. Assets, and particularly information assets, are the focus of security efforts; they are what those efforts are attempting to protect.

Attack: An intentional or unintentional act that can cause damage to or otherwise compromise information and/or the systems that support it. Attacks can be active or passive, intentional or unintentional, and direct or indirect. Someone casually reading sensitiveinformation not intended for his or her use is a passive attack. A hacker attempting to break into an information system is an intentional attack. A lightning strike that causes a fire in a building is an unintentional attack. A direct attack is a hacker using a personal computer to break into a system. An indirect attack is a hacker compromising a system and using it to attack other systems, for example, as part of a botnet (slang for robot network).

This group of compromised computers, running software of the attacker's choosing, can operate autonomously or under the attacker's direct control to attack systems and steal user information or conduct distributed denial-of-service attacks. Direct attacks originate from the threat itself. Indirect attacks originate from a compromised system or resource that is malfunctioning or working under the control of a threat.

Control, safeguard, or **countermeasure:** Security mechanisms, policies, or procedures that can successfully counter attacks, reduce risk, resolve vulnerabilities, and otherwise improve the security within an organization. The various levels and types of controls are discussed more fully in the following chapters.

Exploit: A technique used to compromise a system. This term can be a verb or a noun. Threat agents may attempt to exploit a system or other information asset by using it illegally for their personal gain. Or, an exploit can be a documented process to take advantage of a vulnerability or exposure, usually in software, that is either inherent in the software or is created by the attacker. Exploits make use of existing software tools or custom-made software components.

Exposure: A condition or state of being exposed. In information security, exposure exists when a vulnerability known to an attacker is present.

Loss: A single instance of an information asset suffering damage or unintended or unauthorized modification or disclosure. When an organization's information is stolen, it has suffered a loss.

Protection profile or **security posture:** The entire set of controls and safeguards, including policy, education, training and awareness, and technology, that the organization implements (or fails to implement) to protect the asset. The terms are sometimes used interchangeably with the term *security program*, although the security program often comprises managerial aspects of security, including planning, personnel, and subordinate programs.

Risk: The probability that something unwanted will happen. Organizations must minimize risk to match their **risk appetite**—the quantity and nature of risk the organization is willing to accept.

Subjects and **objects:** A computer can be either the **subject** of an attack—an agent entity used to conduct the attack—or the **object** of an attack—the target entity, as shown in Figure 1-5. A computer can be both the subject and object of an attack, when, for example, it is compromised by an attack (object), and is then used to attack other systems (subject).

Threat: A category of objects, persons, or other entities that presents a danger to an asset. Threats are always present and can be purposeful or undirected. For example, hackers purposefully threaten unprotected information systems, while severe storms incidentally threaten buildings and their contents.

Threat agent: The specific instance or a component of a threat. For example, all hackers

in the world present a collective threat, while Kevin Mitnick, who was convicted for hacking into phone systems, is a specific threat agent. Likewise, a lightning strike, hailstorm, or tornado is a threat agent that is part of the threat of severe storms.

Vulnerability: A weaknesses or fault in a system or protection mechanism that opens it to attack or damage. Some examples of vulnerabilities are a flaw in a software package, an unprotected system port, and an unlocked door. Some **well-known vulnerabilities** have been examined, documented, and published; others remain latent (or undiscovered).

Critical Characteristics of Information

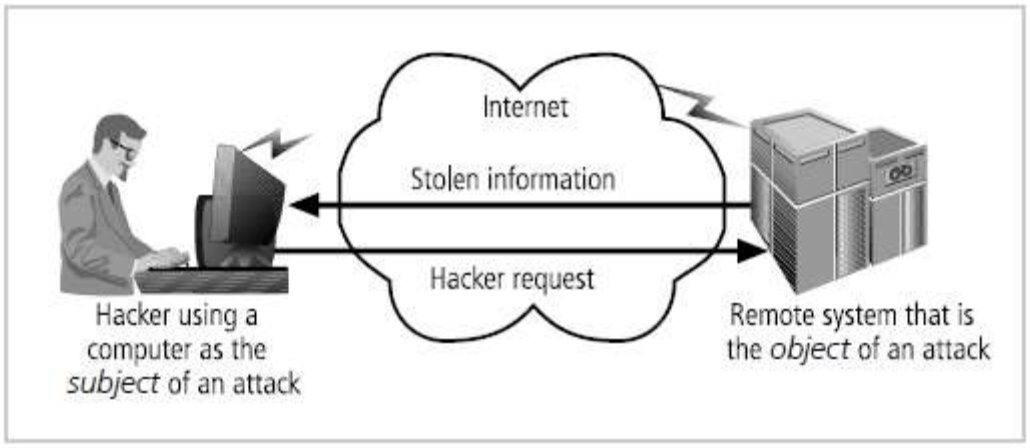


Figure 1-5 Computer as the Subject and Object of an Attack

Each critical characteristic of information—that is, the expanded C.I.A. triangle—is defined in the sections below.

Availability Availability enables authorized users—persons or computer systems—to access information without interference or obstruction and to receive it in the required format. Consider, for example, research libraries that require identification before entrance. Librarians protect the contents of the library so that they are available only to authorized patrons. The librarian must accept a patron's identification before that patron has free access to the book stacks. Once authorized patrons have access to the contents of the stacks, they expect to find the information they need available in a useable format and familiar language,

which in this case typically means bound in a book and written in English.

Accuracy Information has **accuracy** when it is free from mistakes or errors and it has the value that the end user expects. If information has been intentionally or unintentionally modified, it is no longer accurate. Consider, for example, a checking account. You assume that the information contained in your checking account is an accurate representation of your finances. Incorrect information in your checking account can result from external or internal errors. If a bank teller, for instance, mistakenly adds or subtracts too much from your account, the value of the information is changed. Or, you may accidentally enter an incorrect amount into your account register. Either way, an inaccurate bank balance could cause you to make mistakes, such as bouncing a check.

Authenticity Authenticity of information is the quality or state of being genuine or original, rather than a reproduction or fabrication. Information is authentic when it is in the same state in which it was created, placed, stored, or transferred. Consider for a moment some common assumptions about e-mail. When you receive e-mail, you assume that a specific individual or group created and transmitted the e-mail—you assume you know the origin of the e-mail. This is not always the case. E-mail spoofing, the act of sending an e-mail message with a modified field, is a problem for many people today, because often the modified field is the address of the originator. Spoofing the sender's address can fool e-mail recipients into thinking that messages are legitimate traffic, thus inducing them to open e-mail they otherwise might not have. Spoofing can also alter data being transmitted across a network, as in the case of user data protocol (UDP) packet spoofing, which can enable the attacker to get access to data stored on computing systems.

Confidentiality Information has **confidentiality** when it is protected from disclosure or exposure to unauthorized individuals or systems. Confidentiality ensures that *only* those with the rights and privileges to access information are able to do so. When unauthorized individuals or systems can view information, confidentiality is breached. To protect the confidentiality of information, you can use a number of measures, including the following:

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

Integrity Information has **integrity** when it is whole, complete, and uncorrupted. The integrity of information is threatened when the information is exposed to corruption damage, destruction, or other disruption of its authentic state. Corruption can occur while information is being stored or transmitted. Many computer viruses and worms are designed with the explicit purpose of corrupting data. For this reason, a key method for detecting a virus or worm is to look for changes in file integrity as shown by the size of the file. Another key method of assuring information integrity is **file hashing**, in which a file is read by a special algorithm that uses the value of the bits in the file to compute a single large number called a **hash value**. The hash value for any combination of bits is unique. If a computer system performs the same hashing algorithm on a file and obtains a different number than the recorded hash value for that file, the file has been compromised and the integrity of the information is lost. Information integrity is the cornerstone of information systems, because information is of no value or use if users cannot verify its integrity.

Utility The **utility** of information is the quality or state of having value for some purpose or end. Information has value when it can serve a purpose. If information is available, but is not in a format meaningful to the end user, it is not useful. For example, to a private citizen U.S. Census data can quickly become overwhelming and difficult to interpret; however, for a politician, U.S. Census data reveals information about the residents in a district, such as their race, gender, and age. This information can help form a politician's next campaign strategy.

Possession The **possession** of information is the quality or state of ownership or control. Information is said to be in one's possession if one obtains it, independent of format or other characteristics. While a breach of confidentiality always results in a breach of possession, a breach of possession does not always result in a breach of confidentiality. For example, assume a company stores its critical customer data using an encrypted file system. An employee who has quit decides to take a copy of the tape backups to sell the customer records to the competition. The removal of the tapes from their secure environment is a breach of possession. But, because the data is encrypted, neither the employee nor anyone else can read it without the proper decryption methods; therefore, there is no breach of confidentiality.

Today, people caught selling company secrets face increasingly stiff fines with the likelihood of jail time. Also, companies are growing more and more reluctant to hire individuals who have demonstrated dishonesty in their past.

1.2 Need for Security

The Need for Security

Whether it be personal or commercial, data is really valuable so it is important to keep it safe. Data is sometimes deleted or corrupted accidentally, but this can also happen as the result of malicious actions. Either way, there are measures we can take to reduce the risk of this happening.

Malicious Actions	Deliberate unauthorised actions intended to cause damage by viewing, deleting, copying or corrupting data
Accidental Damage	Unintended corruption, deletion or damage to data that is usually caused by human error
Data Corruption	Data corruption refers to errors in computer data that happen during writing, reading, storage, transmission, or processing, which create unintended changes to the original data

Reducing the risk of accidental damage or malicious actions on a local level

- Setting suitable access rights/user permissions, e.g. only allow staff to read/edit/delete the files that are required for their job
- Password protecting individual files
- Running regular backups, to another device or the cloud
- Quality staff training
- Monitoring of staff computer activity
- Locking workstations when unattended
- Sensible naming of files
- Limiting the use of USB ports and email attachments
- Saving work on a regular basis in case of unexpected shutdown
- Use correct shutdown and start up procedures
- Keep storage devices in a safe place
- Set data to read only to prevent accidental editing

The internet and security

The internet has created many additional opportunities for malicious damage to occur to our data or the online systems we use. This is not surprising due to our reliance on the internet and the amount of data we disclose over it.

These additional wider threats include:

- Hacking
- Malware (viruses and spyware)
- Phishing
- Pharming
- DOS Attacks

Reducing the wider risk of malicious actions through the internet

- Install anti-virus/anti-malware/anti-hacking software
- Keep all software, including operating systems, up to date
- Use strong passwords and vary these for different websites
- Don't download software from unknown sources
- Be careful when opening email attachments and don't click suspicious links
- Make sure you are protected by a firewall
- Watch out for the clues, like poor system performance

Need Of Information Security

Information system means to consider available countermeasures or controls stimulated through uncovered vulnerabilities and identify an area where more work is needed. The purpose of data security management is to make sure business continuity and scale back business injury by preventing and minimizing the impact of security incidents. The basic principle of Information Security is:

- **Confidentially**
- **Authentication**
- **Non-Repudiation**
- **Integrity**

The need for Information security:

1. Protecting the functionality of the organization:
   The decision maker in organizations must set policy and operates their organization in compliance with the complex, shifting legislation, efficient and capable applications.
2. Enabling the safe operation of applications:
   The organization is under immense pressure to acquire and operates integrated, efficient and capable applications. The modern organization needs to create an environment that

safeguards application using the organizations IT systems, particularly those application that serves as important elements of the infrastructure of the organization.

3. Protecting the data that the organization collect and use: Data in the organization can be in two forms are either in rest or in motion, the motion of data signifies that data is currently used or processed by the system. The values of the data motivated the attackers to seal or corrupts the data. This is essential for the integrity and the values of the organization's data. Information security ensures the protection of both data in motion as well as data in rest.
4. Safeguarding technology assets in organizations: The organization must add intrastate services based on the size and scope of the organization. Organizational growth could lead to the need for public key infrastructure, PKI an integrated system of the software, encryption methodologies. The information security mechanism used by large organizations is complex in comparison to a small organization. The small organization generally prefers symmetric key encryption of data.

1.3 Security Approaches

In order to determine the safety of data from potential violations and cyber-attacks, the implementation of the security model has an important phase to be carried out. In order to ensure the integrity of the security model can be designed using two methods:

1.Bottom-UpApproach:

The company's security model is applied by system administrators or people who are working in network security or as cyber-engineers. The main idea behind this approach is for individuals working in this field of information systems to use their knowledge and experience in cybersecurity to guarantee the design of a highly secure information security model.

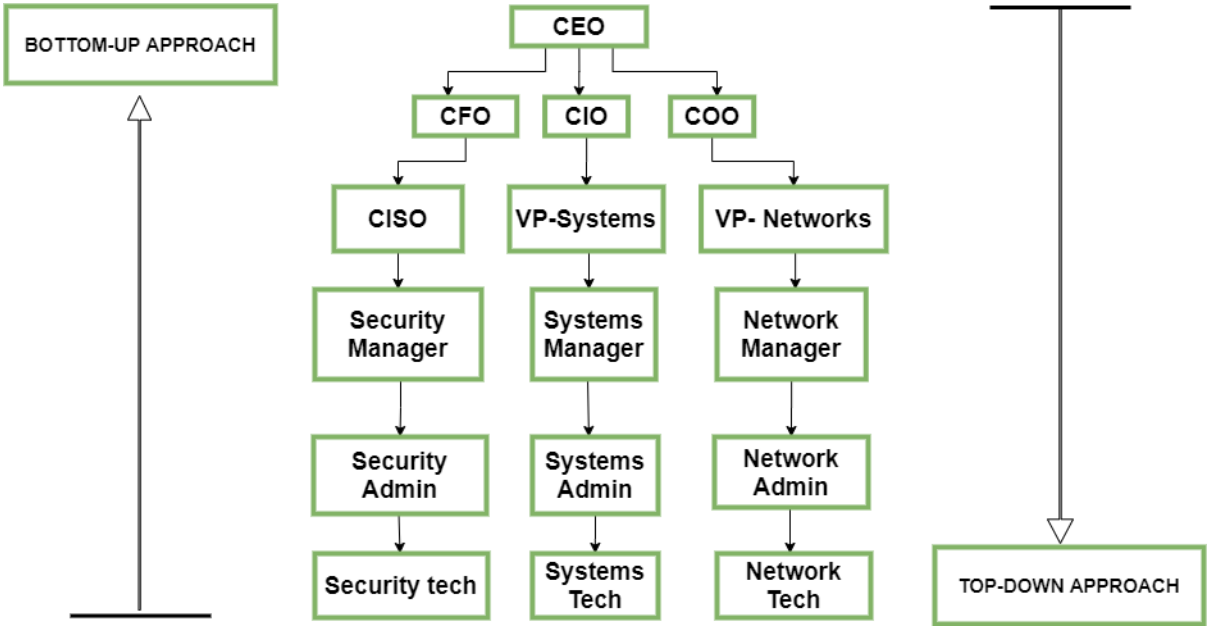
- KeyAdvantages –
  An individual's technical expertise in their field ensures that every system vulnerability is addressed and that the security model is able to counter any potential threats possible.
- Disadvantage –
  Due to the lack of cooperation between senior managers and relevant directives, it is often not suitable for the requirements and strategies of the organisation.

2.Top-DownApproach:

This type of approach is initialized and initiated by the executives of the organization.

- They formulate policies and outline the procedures to be followed.
- Determine the project's priorities and expected results
- Determine liability for every action needed

It is more likely to succeed. That strategy usually provides strong support from top management by committing resources, a consistent preparation and execution mechanism and opportunities to affect corporate culture.



Security management issues have been handled by organizations in various ways. Traditionally, companies adopted a bottom-up approach, where the process is initiated by operational employees and their results are subsequently propagated to upper management as per the proposed policies. Since management has no information about the threat, the effects, the idea of resources, possible returns and the security method, this approach has occasionally created a sudden and violent collapse.

On the contrary, the top-down approach is a highly successful reverse view of the whole issue. Management understands the gravity and

starts the process, which is subsequently collected systematically from cyber engineers and operating personnel.

1.4 Principles of Security

CNSS Security Model

The definition of information security presented in this text is based in part on the CNSS documentcalled the National Training Standard for Information Systems Security Professionals NSTISSI No. 4011. (See www.cnss.gov/Assets/pdf/nstissi_4011.pdf. Since this document waswritten, the NSTISSC was renamed the Committee on National Security Systems (CNSS)— see www.cnss.gov. The library of documents is being renamed as the documents are rewritten.) This document presents a comprehensive information security model and has become a widely accepted evaluation standard for the security of information systems. The model, created by John McCumber in 1991, provides a graphical representation of the architectural approach widely used in computer and information security; it is now known as the McCumber Cube.17 The McCumber Cube in Figure 1-6, shows three dimensions. If extrapolated, the three dimensions of each axis become a 3 3 3 cube with 27 cells representing areas that must be addressed to secure today's information systems. To ensure system security, each of the 27 areas must be properly addressed during the security process. For example, the intersection between technology, integrity, and storage requires a control or safeguard that addresses the need to use technology to protect the integrity of information while in storage. One such control might be a system for detecting host intrusion that protects the integrity of information by alerting the security administrators to the potential modification of a critical file. What is commonly left out of such a model is the need for guidelines and policies that provide direction for the practices and implementations of technologies.

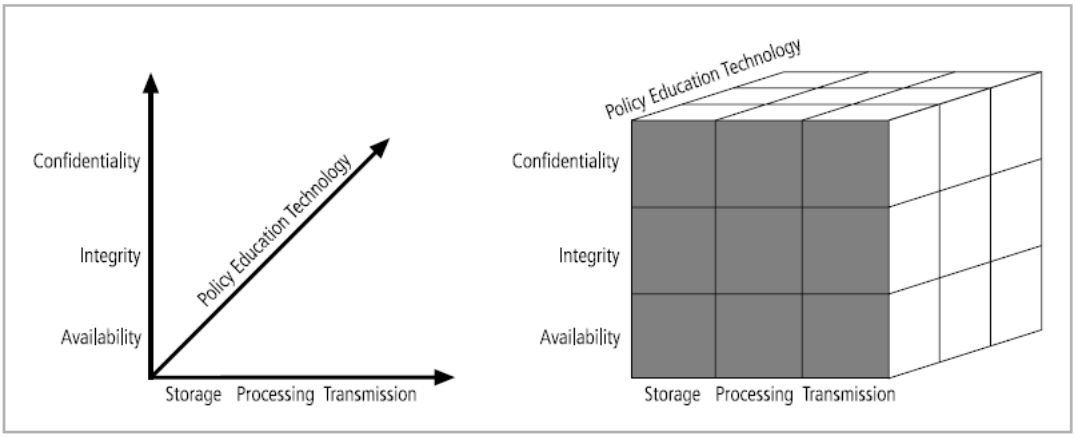


Figure 1-6 The McCumber Cube[18]

Source: Course Technology/Cengage Learning

1.4 Components of an Information System

As shown in Figure 1-7, an information system (IS) is much more than computer hardware; it is the entire set of software, hardware, data, people, procedures, and networks that make possible the use of information resources in the organization. These six critical components enable information to be input, processed, output, and stored. Each of these IS components has its own strengths and weaknesses, as well as its own characteristics and uses. Each component of the information system also has its own security requirements.

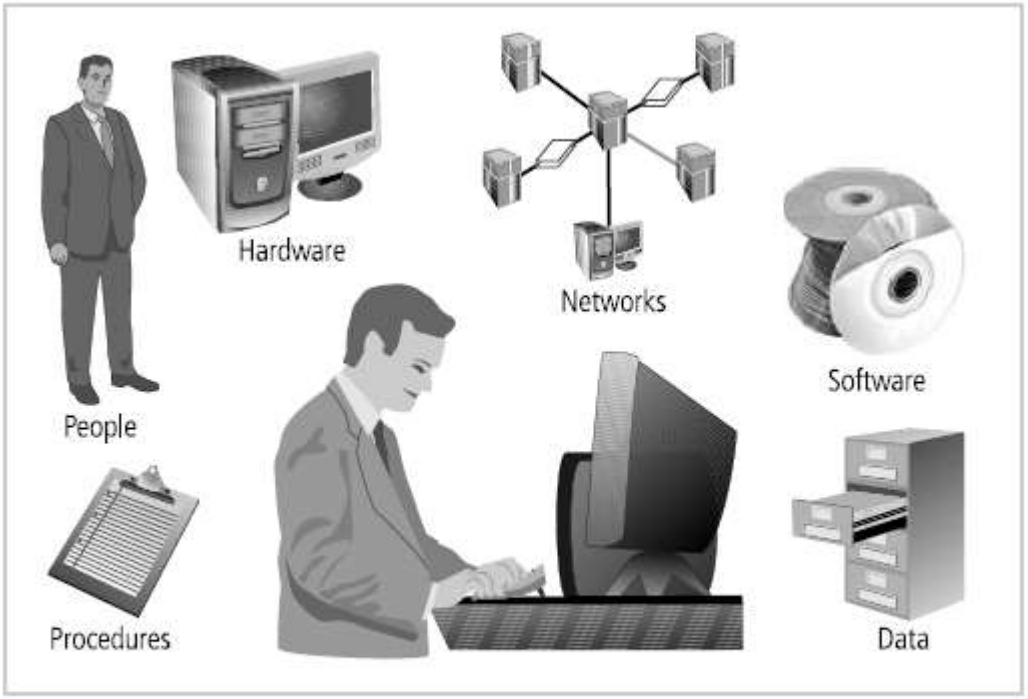


Figure 1-7 Components of an Information System

Source: Course Technology/Cengage Learning

Software

The software component of the IS comprises applications, operating systems, and assorted command utilities. Software is perhaps the most difficult IS component to secure. The exploitation of errors in software programming accounts for a substantial portion of the attacks on information. The information technology industry is rife with reports warning of holes, bugs, weaknesses, or other fundamental problems in software. In fact, many facets of daily life are affected by buggy software, from smartphones that crash to flawed automotive control computers that lead to recalls. Software carries the lifeblood of information through an organization. Unfortunately, software programs are often created under the constraints of project management, which limit time, cost, and manpower. Information security is all too often implemented as an afterthought, rather than developed as an integral component from the beginning. In this way, software programs become an easy target of accidental or intentional attacks.

Hardware

Hardware is the physical technology that houses and executes the software, stores and transports the data, and provides interfaces for the entry and removal of information from the

system. Physical security policies deal with hardware as a physical asset and with the protection of physical assets from harm or theft. Applying the traditional tools of physical security, such as locks and keys, restricts access to and interaction with the hardware components of an information system. Securing the physical location of computers and the computers themselves is important because a breach of physical security can result in a loss of information. Unfortunately, most information systems are built on hardware platforms that cannot guarantee any level of information security if unrestricted access to the hardware is possible.

Before September 11, 2001, laptop thefts in airports were common. A two-person team worked to steal a computer as its owner passed it through the conveyor scanning devices. The first perpetrator entered the security area ahead of an unsuspecting target and quickly went through. Then, the second perpetrator waited behind the target until the target placed his/her computer on the baggage scanner. As the computer was whisked through, the second agent slipped ahead of the victim and entered the metal detector with a substantial collection of keys, coins, and the like, thereby slowing the detection process and allowing the first perpetrator to grab the computer and disappear in a crowded walkway.

While the security response to September 11, 2001 did tighten the security process at airports, hardware can still be stolen in airports and other public places. Although laptops and notebook computers are worth a few thousand dollars, the information contained in them can be worth a great deal more to organizations and individuals.

Data

Data stored, processed, and transmitted by a computer system must be protected. Data is often the most valuable asset possessed by an organization and it is the main target of intentional attacks. Systems developed in recent years are likely to make use of database management systems. When done properly, this should improve the security of the data and the application. Unfortunately, many system development projects do not make full use of the database management system's security capabilities, and in some cases the database is implemented in ways that are less secure than traditional file systems.

People

Though often overlooked in computer security considerations, people have always been a threat to information security. Legend has it that around 200 B.C. a great army threatened the security and stability of the Chinese empire. So ferocious were the invaders that the Chinese emperor commanded the construction of a great wall that would defend against the Hun invaders. Around 1275 A.D., Kublai Khan finally achieved what the Huns had been trying for

thousands of years. Initially, the Khan's army tried to climb over, dig under, and break through the wall. In the end, the Khan simply bribed the gatekeeper—and the rest is history. Whether this event actually occurred or not, the moral of the story is that people can be the weakest link in an organization's information security program. And unless policy, education and training, awareness, and technology are properly employed to prevent people from accidentally or intentionally damaging or losing information, they will remain the weakest link. Social engineering can prey on the tendency to cut corners and the commonplace nature of human error. It can be used to manipulate the actions of people to obtain access information about a system.

Procedures

Another frequently overlooked component of an IS is procedures. Procedures are written instructions for accomplishing a specific task. When an unauthorized user obtains an organization's procedures, this poses a threat to the integrity of the information. For example, a consultant to a bank learned how to wire funds by using the computer center's procedures, which were readily available. By taking advantage of a security weakness (lack of authentication), this bank consultant ordered millions of dollars to be transferred by wire to his own account. Lax security procedures caused the loss of over ten million dollars before the situation was corrected. Most organizations distribute procedures to their legitimate employees so they can access the information system, but many of these companies often fail to provide proper education on the protection of the procedures. Educating employees about safeguarding procedures is as important as physically securing the information system. After all, procedures are information in their own right. Therefore, knowledge of procedures, as with all critical information, should be disseminated among members of the organization only on a need-to-know basis.

Networks

The IS component that created much of the need for increased computer and information security is networking. When information systems are connected to each other to form local area networks (LANs), and these LANs are connected to other networks such as the Internet, new security challenges rapidly emerge. The physical technology that enables network functions is becoming more and more accessible to organizations of every size. Applying the traditional tools of physical security, such as locks and keys, to restrict access to and interaction with the hardware components of an information system are still important; but when computer systems are networked, this approach is no longer enough. Steps to provide network

Balancing Security & Access –

Balancing Information Security and Access

Even with the best planning and implementation, it is impossible to obtain perfect information security. Recall James Anderson's statement from the beginning of this chapter, which emphasizes the need to balance security and access. Information security cannot be absolute: it is a process, not a goal. It is possible to make a system available to anyone, anywhere, anytime, through any means. However, such unrestricted access poses a danger to the security of the information. On the other hand, a completely secure information system would not allow anyone access. For instance, when challenged to achieve a TCSEC C-2 level security certification for its Windows operating system, Microsoft had to remove all networking components and operate the computer from only the console in a secured room. To achieve balance—that is, to operate an information system that satisfies the user and the security professional—the security level must allow reasonable access, yet protect against threats. Figure 1-8 shows some of the competing voices that must be considered when balancing information security and access. Because of today's security concerns and issues, an information system or data-processing department can get too entrenched in the management and protection of systems. An imbalance can occur when the needs of the end user are undermined by too heavy a focus on protecting and administering the information systems. Both information security technologists and end users must recognize that both groups share the same overall goals of the organization—to ensure the data is available when, where, and how it is needed, with

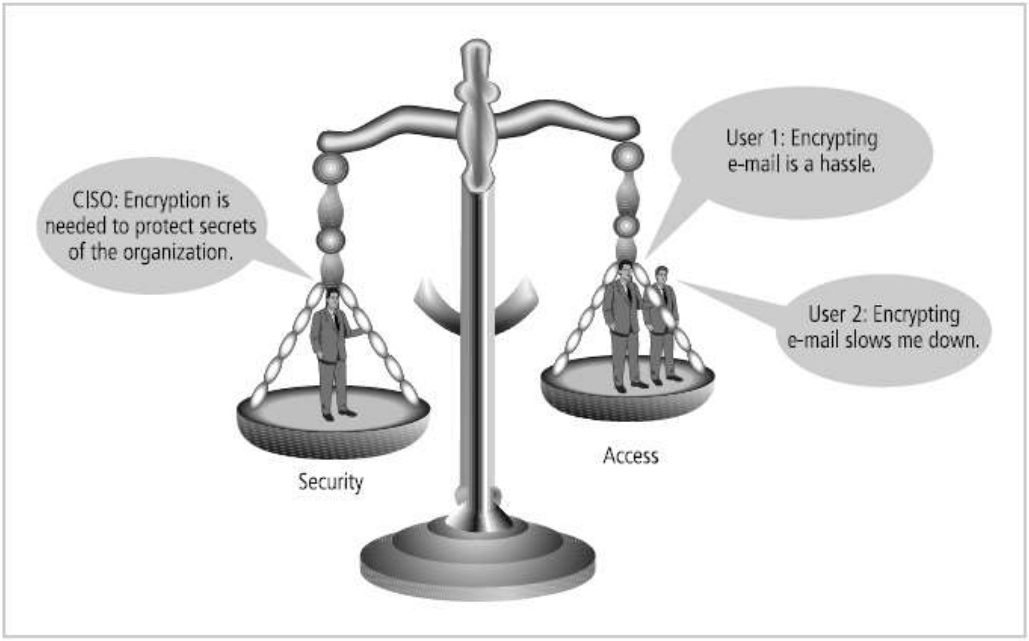


Figure 1-8 Balancing Information Security and Access

Source: Course Technology/Cengage Learning

minimal delays or obstacles. In an ideal world, this level of availability can be met even after concerns about loss, damage, interception, or destruction have been addressed.

Software Development Life Cycle –

The Systems Development Life Cycle

Information security must be managed in a manner similar to any other major system implemented in an organization. One approach for implementing an information security system in

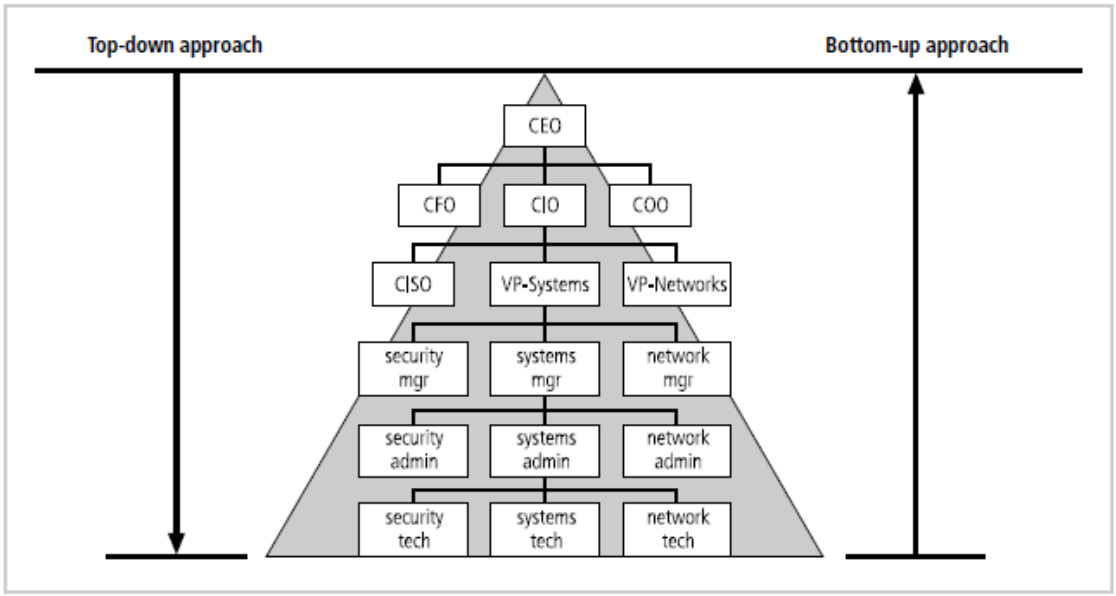


Figure 1-9 Approaches to Information Security Implementation

an organization with little or no formal security in place is to use a variation of the systems development life cycle (SDLC): the security systems development life cycle (SecSDLC). To understand a *security* systems development life cycle, you must first understand the basics of the method upon which it is based.

Methodology and Phases

The **systems development life cycle (SDLC)** is a methodology for the design and implementation of an information system. A **methodology** is a formal approach to solving a problem by means of a structured sequence of procedures. Using a methodology ensures a rigorous process with a clearly defined goal and increases the probability of success. Once a methodology has been adopted, the key milestones are established and a team of individuals is selected and made accountable for accomplishing the project goals.

The traditional SDLC consists of six general phases. If you have taken a system analysis and design course, you may have been exposed to a model consisting of a different number of phases. SDLC models range from having three to twelve phases, all of which have been mapped into the six presented here. The **waterfall model** pictured in Figure 1-10 illustrates that each phase begins with the results and information gained from the previous phase.

At the end of each phase comes a structured review or reality check, during which the team determines if the project should be continued, discontinued, outsourced, postponed, or returned to an earlier phase depending on whether the project is proceeding as expected and on the need for additional expertise, organizational knowledge, or other resources.

Once the system is implemented, it is maintained (and modified) over the remainder of its operational life. Any information systems implementation may have multiple iterations as the cycle is repeated over time. Only by means of constant examination and renewal ca any system, especially an information security program, perform up to expectations in the constantly changing environment in which it is placed.
The following sections describe each phase of the traditional SDLC.20

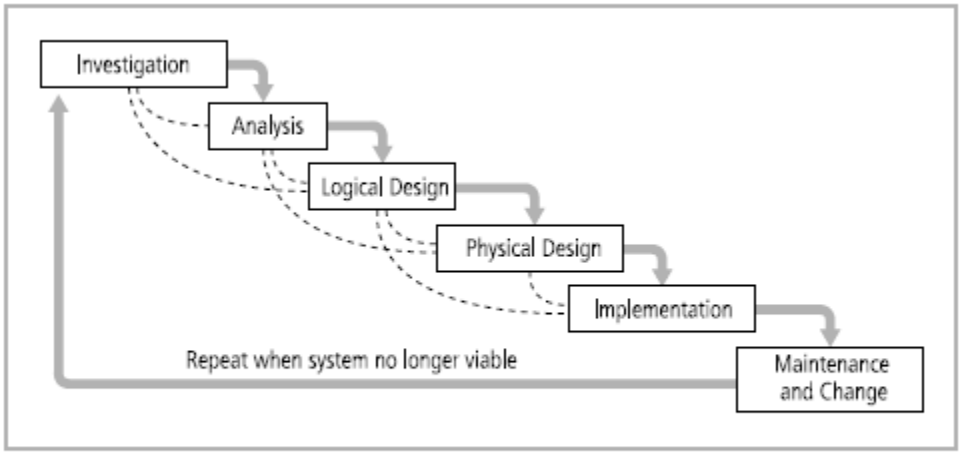


Figure 1-10 SDLC Waterfall Methodology

Source: Course Technology/Cengage Learning

Investigation

The first phase, investigation, is the most important. What problem is the system being developed
to solve? The investigation phase begins with an examination of the event or plan that initiates the process. During the investigation phase, the objectives, constraints, and scope of the project are specified. A preliminary cost-benefit analysis evaluates the perceived benefits and the appropriate levels of cost for those benefits. At the conclusion of this phase, and at every phase following, a feasibility analysis assesses the economic, technical, and behavioral feasibilities of the process and ensures that implementation is worth the organization's time and effort.

Analysis

The analysis phase begins with the information gained during the investigation phase. This phase consists primarily of assessments of the organization, its current systems, and its capability

to support the proposed systems. Analysts begin by determining what the new system is expected to do and how it will interact with existing systems. This phase ends with the documentation of the findings and an update of the feasibility analysis.

Logical Design

In the logical design phase, the information gained from the analysis phase is used to begin creating a systems solution for a business problem. In any systems solution, it is imperative that the first and driving factor is the business need. Based on the business need, applications are selected to provide needed services, and then data support and structures capable of providing the needed inputs are chosen. Finally, based on all of the above, specific technologies to implement the physical solution are delineated. The logical design is, therefore, the blueprint for the desired solution. The logical design is implementation independent, meaning that it contains no reference to specific technologies, vendors, or products. It addresses, instead, how the proposed system will solve the problem at hand. In this stage, analysts generate a number of alternative solutions, each with corresponding strengths and weaknesses, and costs and benefits, allowing for a general comparison of available options. At the end of this phase, another feasibility analysis is performed.

Physical Design

During the physical design phase, specific technologies are selected to support the alternatives identified and evaluated in the logical design. The selected components are evaluated based on a make-or-buy decision (develop the components in-house or purchase them from a vendor). Final designs integrate various components and technologies. After yet another feasibility analysis, the entire solution is presented to the organizational management for approval.

Implementation

In the implementation phase, any needed software is created. Components are ordered, received, and tested. Afterward, users are trained and supporting documentation created. Once all components are tested individually, they are installed and tested as a system. Again a feasibility analysis is prepared, and the sponsors are then presented with the system for a performance review and acceptance test.

Maintenance and Change

The maintenance and change phase is the longest and most expensive phase of the process. This phase consists of the tasks necessary to support and modify the system for the remainder of its useful life cycle. Even though formal development may conclude during this phase, the life cycle of the project continues until it is determined that the process should begin again

from the investigation phase. At periodic points, the system is tested for compliance, and the feasibility of continuance versus discontinuance is evaluated. Upgrades, updates, and patches are managed. As the needs of the organization change, the systems that support the organization must also change. It is imperative that those who manage the systems, as well as those who support them, continually monitor the effectiveness of the systems in relation to the organization's environment. When a current system can no longer support the evolving mission of the organization, the project is terminated and a new project is implemented.

Securing the SDLC

Each of the phases of the SDLC should include consideration of the security of the system being assembled as well as the information it uses. Whether the system is custom and built from scratch, is purchased and then customized, or is commercial off-the-shelf software (COTS), the implementing organization is responsible for ensuring it is used securely. This means that each implementation of a system is secure and does not risk compromising the confidentiality, integrity, and availability of the organization's information assets. The following section, adapted from NIST Special Publication 800-64, rev. 1, provides an overview of the security considerations for each phase of the SDLC. Each of the example SDLC phases [discussed earlier] includes a minimum set of security steps needed to effectively incorporate security into a system during its development. An organization will either use the general SDLC described [earlier] or will have developed a tailored SDLC that meets their specific needs. In either case, NIST recommends that organizations incorporate the associated IT security steps of this general SDLC into their development process:

Investigation/Analysis Phases

Security categorization—defines three levels (i.e., low, moderate, or high) of potential impact on organizations or individuals should there be a breach of security (a loss of confidentiality, integrity, or availability). Security categorization standards assist organizations in making the appropriate selection of security controls for their information systems.

Preliminary risk assessment—results in an initial description of the basic security needs of the system. A preliminary risk assessment should define the threat environment in which the system will operate.

Logical/Physical Design Phases

Risk assessment—analysis that identifies the protection requirements for the system through a formal risk assessment process. This analysis builds on the initial risk assessment performed during the Initiation phase, but will be more in-depth and specific.

Security functional requirements analysis—analysis of requirements that may include the following components:

(1) system security environment (i.e., enterprise information security policy and enterprise security architecture) and

(2) security functional requirements Security assurance requirements analysis—analysis of requirements that address the developmental activities required and assurance evidence needed to produce the desired level of confidence that the information security will work correctly and effectively.

The analysis, based on legal and functional security requirements, will be used as the basis for determining how much and what kinds of assurance are required.

Cost considerations and reporting—determines how much of the development cost can be attributed to information security over the life cycle of the system.

These costs include hardware, software, personnel, and training.

Security planning—ensures that agreed upon security controls, planned or in place, are fully documented. The security plan also provides a complete characterization or description of the information system as well as attachments or references to key documents supporting the agency's information security program (e.g., configuration management plan, contingency plan, incident response plan, security awareness and training plan, rules of behavior, risk assessment, security test and evaluation results, system interconnection agreements, security authorizations/ accreditations, and plan of action and milestones).

Security control development—ensures that security controls described in the respective security plans are designed, developed, and implemented. For information systems currently in operation, the security plans for those systems may call for the development of additional security controls to supplement the controls already in place or the modification of selected controls that are deemed to be less than effective.

Developmental security test and evaluation—ensures that security controls developed for a new information system are working properly and are effective. Some types of security controls (primarily those controls of a non-technical nature) cannot be tested and evaluated until the information system is deployed—these controls are typically management and operational controls.

Other planning components—ensures that all necessary components of the development process are considered when incorporating security into the life cycle. These components include selection of the appropriate contract type, participation

by all necessary functional groups within an organization, participation by the certifier and accreditor, and development and execution of necessary contracting plans and processes.

Implementation Phase

Inspection and acceptance—ensures that the organization validates and verifies that the functionality described in the specification is included in the deliverables.

System integration—ensures that the system is integrated at the operational site where the information system is to be deployed for operation. Security control settings and switches are enabled in accordance with vendor instructions and available security implementation guidance.

Security certification—ensures that the controls are effectively implemented through established verification techniques and procedures and gives organization officials confidence that the appropriate safeguards and countermeasures are in place to protect the organization's information system. Security certification also uncovers and describes the known vulnerabilities in the information system.

Security accreditation—provides the necessary security authorization of an information system to process, store, or transmit information that is required. This authorization is granted by a senior organization official and is based on the verified effectiveness of security controls to some agreed upon level of assurance and an identified residual risk to agency assets or operations.

Maintenance and Change Phase

Configuration management and control—ensures adequate consideration of the potential security impacts due to specific changes to an information system or its surrounding environment. Configuration management and configuration control procedures are critical to establishing an initial baseline of hardware, software, and firmware components for the information system and subsequently controlling and maintaining an accurate inventory of any changes to the system.

Continuous monitoring—ensures that controls continue to be effective in their application through periodic testing and evaluation. Security control monitoring (i.e., verifying the continued effectiveness of those controls over time) and reporting the security status of the information system to appropriate agency officials is an essential activity of a comprehensive information security program.

Information preservation—ensures that information is retained, as necessary, to

conform to current legal requirements and to accommodate future technology changes that may render the retrieval method obsolete.

Media sanitization—ensures that data is deleted, erased, and written over as necessary.

Hardware and software disposal—ensures that hardware and software is disposed of as directed by the information system security officer.

Adapted from Security Considerations in the Information System Development Life Cycle.21

It is imperative that information security be designed into a system from its inception, rather than added in during or after the implementation phase. Information systems that were designed with no security functionality, or with security functions added as an afterthought, often require constant patching, updating, and maintenance to prevent risk to the systems and information. It is a well-known adage that "an ounce of prevention is worth a pound of cure." With this in mind, organizations are moving toward more security-focused development approaches, seeking to improve not only the functionality of the systems they have in place, but consumer confidence in their products. In early 2002, Microsoft effectively suspended development work on many of its products while it put its OS developers, testers, and program managers through an intensive program focusing on secure software development.

It also delayed release of its flagship server operating system to address critical security issues. Many other organizations are following Microsoft's recent lead in putting security into the development process.

Security Systems Development Life Cycle –

The same phases used in the traditional SDLC can be adapted to support the implementation of an information security project. While the two processes may differ in intent and specific activities, the overall methodology is the same. At its heart, implementing information security involves identifying specific threats and creating specific controls to counter those threats. The SecSDLC unifies this process and makes it a coherent program rather than a series of random, seemingly unconnected actions. (Other organizations use a risk management approach to implement information security systems.

Investigation

The investigation phase of the SecSDLC begins with a directive from upper management, dictating the process, outcomes, and goals of the project, as well as its budget and other constraints. Frequently, this phase begins with an **enterprise information security policy (EISP)**, which outlines the implementation of a security program within the organization. Teams of responsible managers, employees, and contractors are organized; problems are analyzed; and the scope of the project, as well as specific goals and objectives and any additional constraints
not covered in the program policy, are defined. Finally, an organizational feasibility analysis is performed to determine whether the organization has the resources and commitment necessary to conduct a successful security analysis and design.

Analysis

In the analysis phase, the documents from the investigation phase are studied. The development team conducts a preliminary analysis of existing security policies or programs, along with that of documented current threats and associated controls. This phase also includes an analysis of relevant legal issues that could affect the design of the security solution. Increasingly, privacy laws have become a major consideration when making decisions about information systems that manage personal information. Recently, many states have implemented
legislation making certain computer-related activities illegal. A detailed understanding of these issues is vital. Risk management also begins in this stage. **Risk management** is the process of identifying, assessing, and evaluating the levels of risk facing the organization, specifically the threats to the organization's security and to the information stored and processed by the organization.

Logical Design

The logical design phase creates and develops the blueprints for information security, and examines and implements key policies that influence later decisions. Also at this stage, the team plans the incident response actions to be taken in the event of partial or catastrophic loss. The planning answers the following questions:

Continuity planning: How will business continue in the event of a loss?

Incident response: What steps are taken when an attack occurs?

Disaster recovery: What must be done to recover information and vital systems immediately after a disastrous event?

Next, a feasibility analysis determines whether or not the project should be continued or be outsourced.

Physical Design

The physical design phase evaluates the information security technology needed to support the blueprint outlined in the logical design generates alternative solutions, and determines a final design. The information security blueprint may be revisited to keep it in line with the changes needed when the physical design is completed. Criteria for determining the definition of successful solutions are also prepared during this phase. Included at this time are the designs for physical security measures to support the proposed technological solutions. At the end of this phase, a feasibility study determines the readiness of the organization for the proposed project, and then the champion and sponsors are presented with the design. At this time, all parties
involved have a chance to approve the project before implementation begins.

Implementation

The implementation phase in of SecSDLC is also similar to that of the traditional SDLC. The security solutions are acquired (made or bought), tested, implemented, and tested again. Personnel issues are evaluated, and specific training and education programs conducted. Finally, the entire tested package is presented to upper management for final approval.

Maintenance and Change

Maintenance and change is the last, though perhaps most important, phase, given the current ever-changing threat environment. Today’s information security systems need constant

Phases	Steps common to both the systems development life cycle and the security systems development life cycle	Steps unique to the security systems development life cycle
Phase 1: Investigation	• Outline project scope and goals • Estimate costs • Evaluate existing resources • Analyze feasibility	• Management defines project processes and goals and documents these in the program security policy
Phase 2: Analysis	• Assess current system against plan developed in Phase 1 • Develop preliminary system requirements • Study integration of new system with existing system • Document findings and update feasibility analysis	• Analyze existing security policies and programs • Analyze current threats and controls • Examine legal issues • Perform risk analysis
Phase 3: Logical Design	• Assess current business needs against plan developed in Phase 2 • Select applications, data support, and structures • Generate multiple solutions for consideration • Document findings and update feasibility analysis	• Develop security blueprint • Plan incident response actions • Plan business response to disaster • Determine feasibility of continuing and/or outsourcing the project
Phase 4: Physical Design	• Select technologies to support solutions developed in Phase 3 • Select the best solution • Decide to make or buy components • Document findings and update feasibility analysis	• Select technologies needed to support security blueprint • Develop definition of successful solution • Design physical security measures to support techno logical solutions • Review and approve project
Phase 5: Implementation	• Develop or buy software • Order components • Document the system • Train users • Update feasibility analysis • Present system to users • Test system and review performance	• Buy or develop security solutions • At end of phase, present tested package to management for approval
Phase 6: Maintenance and Change	• Support and modify system during its useful life • Test periodically for compliance with business needs • Upgrade and patch as necessary	• Constantly monitor, test, modify, update, and repair to meet changing threats

Table 1-2 SDLC and SecSDLC Phase Summary

monitoring, testing, modification, updating, and repairing. Applications systems developed within the framework of the traditional SDLC are not designed to anticipate a software attack that requires some degree of application reconstruction. In information security, the battle for stable, reliable systems is a defensive one. Often, repairing damage and restoring information is a constant effort against an unseen adversary. As new threats emerge and old threats evolve, the information security profile of an organization must constantly adapt to prevent threats from successfully penetrating sensitive data. This constant vigilance and security can be compared to that of a fortress where threats from outside as well as from within must be constantly monitored and checked with continuously new and more innovative technologies.

Table 1-2 summarizes the steps performed in both the systems development life cycle and the security systems development life cycle. Since the security systems development life cycle is based on the systems development life cycle, the steps in the cycles are similar, and thus those common to both cycles are outlined in column 2. Column 3 shows the steps unique to the security systems development life cycle that are performed in each phase.

It takes a wide range of professionals to support a diverse information security program. As noted earlier in this chapter, information security is best initiated from the top down. Senior management is the key component and the vital force for a successful implementation of an information security program. But administrative support is also essential to developing and executing specific security policies and procedures, and technical expertise is of course essential to implementing the details of the information security program. The following sections describe the typical information security responsibilities of various professional roles in an organization.

Senior Management

The senior technology officer is typically the chief information officer (CIO), although other titles such as vice president of information, VP of information technology, and VP of systems may be used. The CIO is primarily responsible for advising the chief executive officer, president, or company owner on the strategic planning that affects the management of information in the organization. The CIO translates the strategic plans of the organization as a whole into strategic information plans for the information systems or data processing division of the organization. Once this is accomplished, CIOs work with subordinate managers to develop tactical and operational plans for the division and to enable planning and management of the systems that support the organization.

The chief information security officer (CISO) has primary responsibility for the assessment, management, and implementation of information security in the organization. The CISO may also be referred to as the manager for IT security, the security administrator, or a similar title. The CISO usually reports directly to the CIO, although in larger organizations it is not uncommon for one or more layers of management to exist between the two. However, the recommendations of the CISO to the CIO must be given equal, if not greater, priority than other technology and information-related proposals. The placement of the CISO and supporting security staff in organizational hierarchies is the subject of current debate across the industry.

Information Security Project Team

The information security project team should consist of a number of individuals who are experienced in one or multiple facets of the required technical and nontechnical areas. Many of the same skills needed to manage and implement security are also needed to design it. Members of the security project team fill the following roles:

Champion: A senior executive who promotes the project and ensures its support, both financially and administratively, at the highest levels of the organization.

Team leader: A project manager, who may be a departmental line manager or staff unit manager, who understands project management, personnel management, and information security technical requirements.

Security policy developers: People who understand the organizational culture, existing policies, and requirements for developing and implementing successful policies.

Risk assessment specialists: People who understand financial risk assessment techniques, the value of organizational assets, and the security methods to be used.

Security professionals: Dedicated, trained, and well-educated specialists in all aspects of information security from both a technical and nontechnical standpoint.

Systems administrators: People with the primary responsibility for administering the systems that house the information used by the organization.

End users: Those whom the new system will most directly affect. Ideally, a selection of users from various departments, levels, and degrees of technical knowledge assist the team in focusing on the application of realistic controls applied in ways that do not disrupt the essential business activities they seek to safeguard.

Data Responsibilities

The three types of data ownership and their respective responsibilities are outlined below:

Data owners: Those responsible for the security and use of a particular set of information. They are usually members of senior management and could be CIOs. The data owners usually determine the level of data classification (discussed later), as well as the changes to that classification required by organizational change. The data owners work with subordinate managers to oversee the day-to-day administration of the data.

Data custodians: Working directly with data owners, data custodians are responsible for the storage, maintenance, and protection of the information. Depending on the size of the organization, this may be a dedicated position, such as the CISO, or it may be an additional responsibility of a systems administrator or other technology manager. The duties of a data custodian often include overseeing data storage and backups, implementing the specific procedures and policies laid out in the security policies and plans, and reporting to the data owner.

Data users: End users who work with the information to perform their assigned roles supporting the mission of the organization. Everyone in the organization is responsible for the

security of data, so data users are included here as individuals with an information security role.