

Introduction to Information Security

Do not figure on opponents not attacking; worry about your own lack of preparation.

BOOK OF THE FIVE RINGS

For Amy, the day began like any other at the Sequential Label and Supply Company (SLS) help desk. Taking calls and helping office workers with computer problems was not glamorous, but she enjoyed the work; it was challenging and paid well. Some of her friends in the industry worked at bigger companies, some at cutting-edge tech companies, but they all agreed that jobs in information technology were a good way to pay the bills.

The phone rang, as it did on average about four times an hour and about 28 times a day. The first call of the day, from a worried user hoping Amy could help him out of a jam, seemed typical. The call display on her monitor gave some of the facts: the user's name, his phone number, the department in which he worked, where his office was on the company campus, and a list of all the calls he'd made in the past.

"Hi, Bob," she said. "Did you get that document formatting problem squared away?"

"Sure did, Amy. Hope we can figure out what's going on this time."

"We'll try, Bob. Tell me about it."

"Well, my PC is acting weird," Bob said. "When I go to the screen that has my e-mail program running, it doesn't respond to the mouse or the keyboard."

"Did you try a reboot yet?"

Not For Sale

Not For Sale

“Sure did. But the window wouldn’t close, and I had to turn it off. After it restarted, I opened the e-mail program, and it’s just like it was before—no response at all. The other stuff is working OK, but really, really slowly. Even my Internet browser is sluggish.”

“OK, Bob. We’ve tried the usual stuff we can do over the phone. Let me open a case, and I’ll dispatch a tech over as soon as possible.”

Amy looked up at the LED tally board on the wall at the end of the room. She saw that there were only two technicians dispatched to deskside support at the moment, and since it was the day shift, there were four available.

“Shouldn’t be long at all, Bob.”

She hung up and typed her notes into ISIS, the company’s Information Status and Issues System. She assigned the newly generated case to the deskside dispatch queue, which would page the roving deskside team with the details in just a few minutes.

A moment later, Amy looked up to see Charlie Moody, the senior manager of the server administration team, walking briskly down the hall. He was being trailed by three of his senior technicians as he made a beeline from his office to the door of the server room where the company servers were kept in a controlled environment. They all looked worried.

Just then, Amy’s screen beeped to alert her of a new e-mail. She glanced down. It beeped again—and again. It started beeping constantly. She clicked on the envelope icon and, after a short delay, the mail window opened. She had 47 new e-mails in her inbox. She opened one from Davey Martinez, an acquaintance from the Accounting Department. The subject line said, “Wait till you see this.” The message body read, “Look what this has to say about our managers’ salaries...” Davey often sent her interesting and funny e-mails, and she failed to notice that the file attachment icon was unusual before she clicked it.

Her PC showed the hourglass pointer icon for a second and then the normal pointer reappeared. Nothing happened. She clicked the next e-mail message in the queue. Nothing happened. Her phone rang again. She clicked the ISIS icon on her computer desktop to activate the call management software and activated her headset. “Hello, Tech Support, how can I help you?” She couldn’t greet the caller by name because ISIS had not responded.

“Hello, this is Erin Williams in receiving.”

Amy glanced down at her screen. Still no ISIS. She glanced up to the tally board and was surprised to see the inbound-call-counter tallying up waiting calls like digits on a stopwatch. Amy had never seen so many calls come in at one time.

“Hi, Erin,” Amy said. “What’s up?”

“Nothing,” Erin answered. “That’s the problem.” The rest of the call was a replay of Bob’s, except that Amy had to jot notes down on a legal pad. She couldn’t dispatch the deskside support team either. She looked at the tally board. It had gone dark. No numbers at all.

Then she saw Charlie running down the hall from the server room. He didn’t look worried anymore. He looked frantic.

Amy picked up the phone again. She wanted to check with her supervisor about what to do now. There was no dial tone.

LEARNING OBJECTIVES:

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

- Define information security
- Recount the history of computer security, and explain how it evolved into information security
- Define key terms and critical concepts of information security
- Enumerate the phases of the security systems development life cycle
- Describe the information security roles of professionals within an organization



Introduction

James Anderson, executive consultant at Emagined Security, Inc., believes information security in an enterprise is a “well-informed sense of assurance that the information risks and controls are in balance.” He is not alone in his perspective. Many information security practitioners recognize that aligning information security needs with business objectives must be the top priority.

This chapter’s opening scenario illustrates that the information risks and controls are not in balance at Sequential Label and Supply. Though Amy works in a technical support role and her job is to solve technical problems, it does not occur to her that a malicious software program, like a worm or virus, might be the agent of the company’s current ills. Management also shows signs of confusion and seems to have no idea how to contain this kind of incident. If you were in Amy’s place and were faced with a similar situation, what would you do? How would you react? Would it occur to you that something far more insidious than a technical malfunction was happening at your company? As you explore the chapters of this book and learn more about information security, you will become better able to answer these questions. But before you can begin studying the details of the discipline of information security, you must first know the history and evolution of the field.

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 (see Figure 1-1), 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 safeguards.

During these early years, information security was a straightforward process composed predominantly of physical security and simple document classification schemes. The primary threats to security were physical theft of equipment, espionage against the products of the systems, and sabotage. One of the first documented security problems that fell outside these categories occurred in the early 1960s, when a systems administrator was working on an MOTD



Earlier versions of the German code machine Enigma were first broken by the Poles in the 1930s. The British and Americans managed to break later, more complex versions during World War II. The increasingly complex versions of the Enigma, especially the submarine or *Unterseeboot* version of the Enigma, caused considerable anguish to Allied forces before finally being cracked. The information gained from decrypted transmissions was used to anticipate the actions of German armed forces. "Some ask why, if we were reading the Enigma, we did not win the war earlier. One might ask, instead, when, if ever, we would have won the war if we hadn't read it."¹

Figure 1-1 The Enigma

Source: Courtesy of National Security Agency

(message of the day) file, and another administrator was editing the password file. A software glitch mixed the two files, and the entire password file was printed on every output file.²

The 1960s

During the Cold War, many more mainframes were brought online to accomplish more complex and sophisticated tasks. It became necessary to enable these mainframes to communicate via a less cumbersome process than mailing magnetic tapes between computer centers. In response to this need, the Department of Defense's Advanced Research Project Agency (ARPA) began examining the feasibility of a redundant, networked communications system to support the military's exchange of information. Larry Roberts, known as the founder of the Internet, developed the project—which was called ARPANET—from its inception. ARPANET is the predecessor to the Internet (see Figure 1-2 for an excerpt from the ARPANET Program Plan).

The 1970s and 80s

During the next decade, ARPANET became popular and more widely used, and the potential for its misuse grew. In December of 1973, Robert M. "Bob" Metcalfe, who is credited

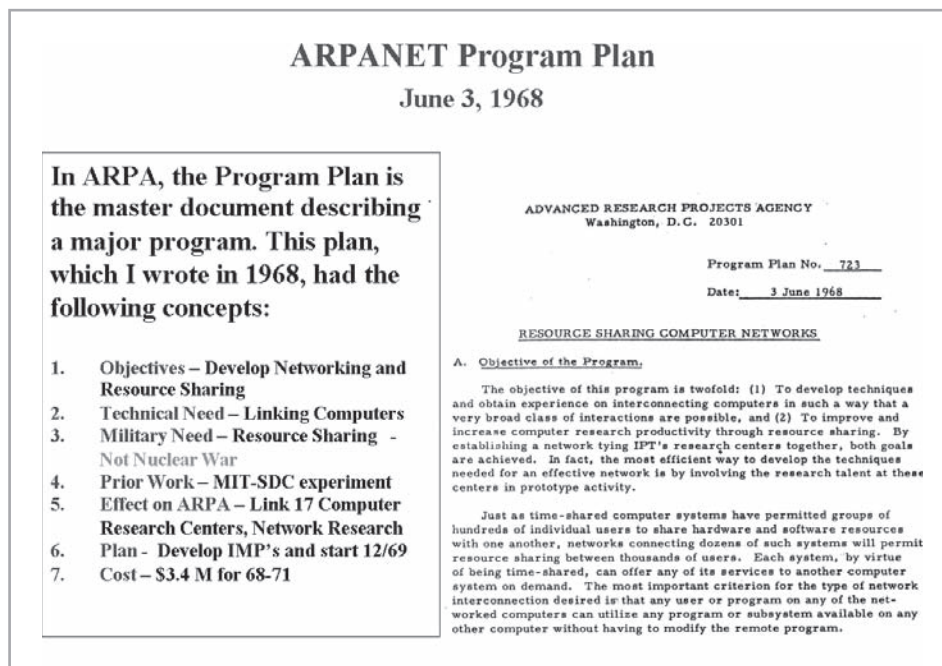


Figure 1-2 Development of the ARPANET Program Plan³

Source: Courtesy of Dr. Lawrence Roberts

with the development of Ethernet, one of the most popular networking protocols, identified fundamental problems with ARPANET security. Individual remote sites did not have sufficient controls and safeguards to protect data from unauthorized remote users. Other problems abounded: vulnerability of password structure and formats; lack of safety procedures for dial-up connections; and nonexistent user identification and authorization to the system. Phone numbers were widely distributed and openly publicized on the walls of phone booths, giving hackers easy access to ARPANET. Because of the range and frequency of computer security violations and the explosion in the numbers of hosts and users on ARPANET, network security was referred to as network insecurity.⁴ In 1978, a famous study entitled “Protection Analysis: Final Report” was published. It focused on a project undertaken by ARPA to discover the vulnerabilities of operating system security. For a timeline that includes this and other seminal studies of computer security, see Table 1-1.

The movement toward security that went beyond protecting physical locations began with a single paper sponsored by the Department of Defense, the Rand Report R-609, which attempted to define the multiple controls and mechanisms necessary for the protection of a multilevel computer system. The document was classified for almost ten years, and is now considered to be the paper that started the study of computer security.

The security—or lack thereof—of the systems sharing resources inside the Department of Defense was brought to the attention of researchers in the spring and summer of 1967. At that time, systems were being acquired at a rapid rate and securing them was a pressing concern for both the military and defense contractors.

Date	Documents
1968	Maurice Wilkes discusses password security in <i>Time-Sharing Computer Systems</i> .
1973	Schell, Downey, and Popek examine the need for additional security in military systems in "Preliminary Notes on the Design of Secure Military Computer Systems." ⁵
1975	The Federal Information Processing Standards (FIPS) examines Digital Encryption Standard (DES) in the <i>Federal Register</i> .
1978	Bisbey and Hollingworth publish their study "Protection Analysis: Final Report," discussing the Protection Analysis project created by ARPA to better understand the vulnerabilities of operating system security and examine the possibility of automated vulnerability detection techniques in existing system software. ⁶
1979	Morris and Thompson author "Password Security: A Case History," published in the Communications of the Association for <i>Computing Machinery</i> (ACM). The paper examines the history of a design for a password security scheme on a remotely accessed, time-sharing system.
1979	Dennis Ritchie publishes "On the Security of UNIX" and "Protection of Data File Contents," discussing secure user IDs and secure group IDs, and the problems inherent in the systems.
1984	Grampp and Morris write "UNIX Operating System Security." In this report, the authors examine four "important handles to computer security": physical control of premises and computer facilities, management commitment to security objectives, education of employees, and administrative procedures aimed at increased security. ⁷
1984	Reeds and Weinberger publish "File Security and the UNIX System Crypt Command." Their premise was: "No technique can be secure against wiretapping or its equivalent on the computer. Therefore no technique can be secure against the systems administrator or other privileged users ... the naive user has no chance." ⁸

Table 1-1 Key Dates for Seminal Works in Early Computer Security

In June of 1967, the Advanced Research Projects Agency formed a task force to study the process of securing classified information systems. The Task Force was assembled in October of 1967 and met regularly to formulate recommendations, which ultimately became the contents of the Rand Report R-609.⁹

The Rand Report R-609 was the first widely recognized published document to identify the role of management and policy issues in computer security. It noted that the wide utilization of networking components in information systems in the military introduced security risks that could not be mitigated by the routine practices then used to secure these systems.¹⁰ This paper signaled a pivotal moment in computer security history—when the scope of computer security expanded significantly from the safety of physical locations and hardware to include the following:

- Securing the data
- Limiting random and unauthorized access to that data
- Involving personnel from multiple levels of the organization in matters pertaining to information security

MULTICS Much of the early research on computer security centered on a system called Multiplexed Information and Computing Service (MULTICS). Although it is now obsolete, MULTICS is noteworthy because it was the first operating system to integrate security into

its core functions. It was a mainframe, time-sharing operating system developed in the mid-1960s by a consortium of General Electric (GE), Bell Labs, and the Massachusetts Institute of Technology (MIT).



In mid-1969, not long after the restructuring of the MULTICS project, several of its developers (Ken Thompson, Dennis Ritchie, Rudd Canaday, and Doug McIlroy) created a new operating system called UNIX. While the MULTICS system implemented multiple security levels and passwords, the UNIX system did not. Its primary function, text processing, did not require the same level of security as that of its predecessor. In fact, it was not until the early 1970s that even the simplest component of security, the password function, became a component of UNIX.

In the late 1970s, the microprocessor brought the personal computer and a new age of computing. The PC became the workhorse of modern computing, thereby moving it out of the data center. This decentralization of data processing systems in the 1980s gave rise to networking—that is, the interconnecting of personal computers and mainframe computers, which enabled the entire computing community to make all their resources work together.

The 1990s

At the close of the twentieth century, networks of computers became more common, as did the need to connect these networks to each other. This gave rise to the Internet, the first global network of networks. The Internet was made available to the general public in the 1990s, having previously been the domain of government, academia, and dedicated industry professionals. The Internet brought connectivity to virtually all computers that could reach a phone line or an Internet-connected local area network (LAN). After the Internet was commercialized, the technology became pervasive, reaching almost every corner of the globe with an expanding array of uses.

Since its inception as a tool for sharing Defense Department information, the Internet has become an interconnection of millions of networks. At first, these connections were based on de facto **standards**, because industry standards for interconnection of networks did not exist at that time. These de facto standards did little to ensure the security of information though as these precursor technologies were widely adopted and became industry standards, some degree of security was introduced. However, early Internet deployment treated security as a low priority. In fact, many of the problems that plague e-mail on the Internet today are the result of this early lack of security. At that time, when all Internet and e-mail users were (presumably trustworthy) computer scientists, mail server authentication and e-mail encryption did not seem necessary. Early computing approaches relied on security that was built into the physical environment of the data center that housed the computers. As networked computers became the dominant style of computing, the ability to physically secure a networked computer was lost, and the stored information became more exposed to security threats.

2000 to Present

Today, the Internet brings millions of unsecured computer networks into continuous communication with each other. The security of each computer's stored information is now contingent on the level of security of every other computer to which it is connected. Recent years have seen a growing awareness of the need to improve information security, as well as a realization that information security is important to national defense. The growing threat of

cyber attacks have made governments and companies more aware of the need to defend the computer-controlled control systems of utilities and other critical infrastructure. There is also growing concern about nation-states engaging in information warfare, and the possibility that business and personal information systems could become casualties if they are undefended.

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 protect its 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

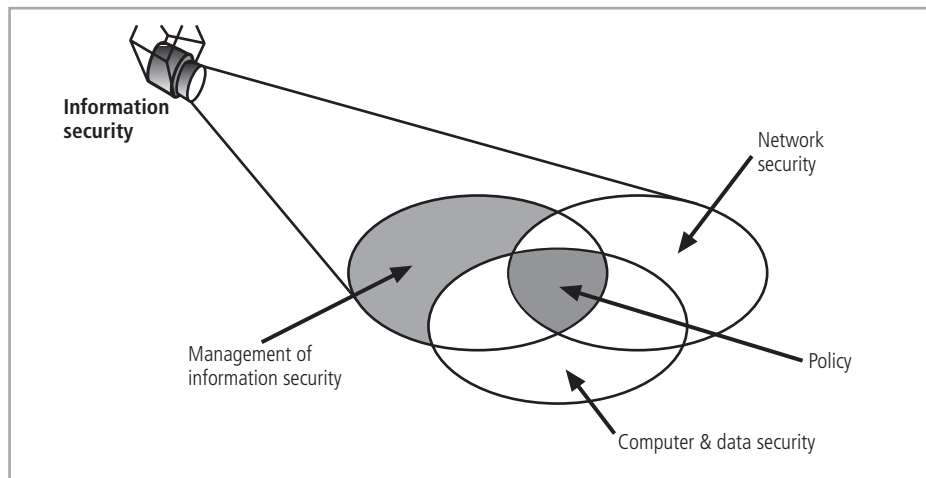


Figure 1-3 Components of Information Security

Source: Course Technology/Cengage Learning

section. C.I.A. triangle terminology is used in this chapter because of the breadth of material that is based on it.

Key Information Security Concepts

This book uses a number of terms and concepts that are essential to any discussion of information security. Some of these terms are illustrated in Figure 1-4; all are covered in greater detail in subsequent chapters.

- **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 sensitive information 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.

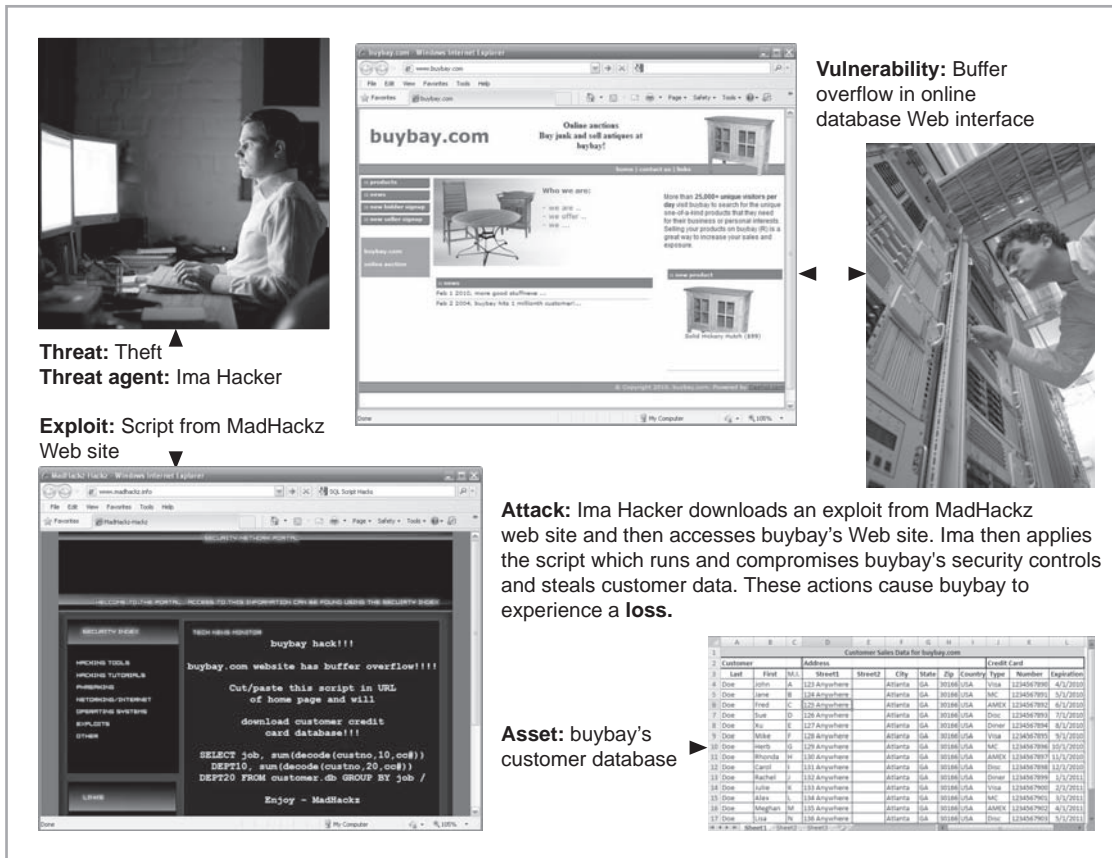


Figure 1-4 Information Security Terms

Source: Course Technology/Cengage Learning

- **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

The value of information comes from the characteristics it possesses. When a characteristic of information changes, the value of that information either increases, or, more commonly, decreases. Some characteristics affect information's value to users more than others do. This can depend on circumstances; for example, timeliness of information can be a critical factor, because information loses much or all of its value when it is delivered too late. Though information security professionals and end users share an understanding of the characteristics of

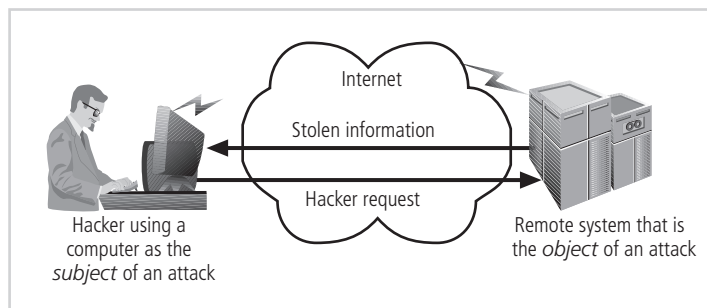


Figure 1-5 Computer as the Subject and Object of an Attack

Source: Course Technology/Cengage Learning

Not For Sale

information, tensions can arise when the need to secure the information from threats conflicts with the end users' need for unhindered access to the information. For instance, end users may perceive a tenth-of-a-second delay in the computation of data to be an unnecessary annoyance. Information security professionals, however, may perceive that tenth of a second as a minor delay that enables an important task, like data encryption. 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.

Another variation on spoofing is **phishing**, when an attacker attempts to obtain personal or financial information using fraudulent means, most often by posing as another individual or organization. Pretending to be someone you are not is sometimes called *pretexting* when it is undertaken by law enforcement agents or private investigators. When used in a phishing attack, e-mail spoofing lures victims to a Web server that does not represent the organization it purports to, in an attempt to steal their private data such as account numbers and passwords. The most common variants include posing as a bank or brokerage company, e-commerce organization, or Internet service provider. Even when authorized, pretexting does not always lead to a satisfactory outcome. In 2006, the CEO of Hewlett-Packard

Corporation, Patricia Dunn, authorized contract investigators to use pretexting to “smokeout” a corporate director suspected of leaking confidential information. The resulting firestorm of negative publicity led to Ms. Dunn’s eventual departure from the company.¹³



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

Confidentiality, like most of the characteristics of information, is interdependent with other characteristics and is most closely related to the characteristic known as privacy. The relationship between these two characteristics is covered in more detail in Chapter 3, “Legal and Ethical Issues in Security.”

The value of confidentiality of information is especially high when it is personal information about employees, customers, or patients. Individuals who transact with an organization expect that their personal information will remain confidential, whether the organization is a federal agency, such as the Internal Revenue Service, or a business. Problems arise when companies disclose confidential information. Sometimes this disclosure is intentional, but there are times when disclosure of confidential information happens by mistake—for example, when confidential information is mistakenly e-mailed to someone *outside* the organization rather than to someone *inside* the organization. Several cases of privacy violation are outlined in Offline: Unintentional Disclosures.

Other examples of confidentiality breaches are an employee throwing away a document containing critical information without shredding it, or a hacker who successfully breaks into an internal database of a Web-based organization and steals sensitive information about the clients, such as names, addresses, and credit card numbers.

As a consumer, you give up pieces of confidential information in exchange for convenience or value almost daily. By using a “members only” card at a grocery store, you disclose some of your spending habits. When you fill out an online survey, you exchange pieces of your personal history for access to online privileges. The bits and pieces of your information that you disclose are copied, sold, replicated, distributed, and eventually coalesced into profiles and even complete dossiers of yourself and your life. A similar technique is used in a criminal enterprise called **salami theft**. A deli worker knows he or she cannot steal an entire salami, but a few slices here or there can be taken home without notice. Eventually the deli worker has stolen a whole salami. In information security, salami theft occurs when an employee steals a few pieces of information at a time, knowing that taking more would be noticed—but eventually the employee gets something complete or useable.

Integrity Information has **integrity** when it is whole, complete, and uncorrupted. The integrity of information is threatened when the information is exposed to corruption,

Offline Unintentional Disclosures

In February 2005, the data aggregation and brokerage firm ChoicePoint revealed that it had been duped into releasing personal information about 145,000 people to identity thieves during 2004. The perpetrators used stolen identities to create ostensibly legitimate business entities, which then subscribed to ChoicePoint to acquire the data fraudulently. The company reported that the criminals opened many accounts and recorded personal information on individuals, including names, addresses, and identification numbers. They did so without using any network or computer-based attacks; it was simple fraud.¹⁴ While the amount of damage has yet to be compiled, the fraud is feared to have allowed the perpetrators to arrange many hundreds of instances of identity theft.

The giant pharmaceutical organization Eli Lilly and Co. released the e-mail addresses of 600 patients to one another in 2001. The American Civil Liberties Union (ACLU) denounced this breach of privacy, and information technology industry analysts noted that it was likely to influence the public debate on privacy legislation.

The company claimed that the mishap was caused by a programming error that occurred when patients who used a specific drug produced by the company signed up for an e-mail service to access support materials provided by the company. About 600 patient addresses were exposed in the mass e-mail.¹⁵

In another incident, the intellectual property of Jerome Stevens Pharmaceuticals, a small prescription drug manufacturer from New York, was compromised when the FDA released documents the company had filed with the agency. It remains unclear whether this was a deliberate act by the FDA or a simple error; but either way, the company's secrets were posted to a public Web site for several months before being removed.¹⁶

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.

File corruption is not necessarily the result of external forces, such as hackers. Noise in the transmission media, for instance, can also cause data to lose its integrity. Transmitting data on a circuit with a low voltage level can alter and corrupt the data. Redundancy bits and check bits can compensate for internal and external threats to the integrity of information. During each transmission, algorithms, hash values, and the error-correcting codes ensure the integrity of the information. Data whose integrity has been compromised is retransmitted.



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.

CNSS Security Model

The definition of information security presented in this text is based in part on the CNSS document called the National Training Standard for Information Systems Security Professionals NSTISSI No. 4011. (See www.cnss.gov/Assets/pdf/nstissi_4011.pdf. Since this document was written, 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 $3 \times 3 \times 3$ 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

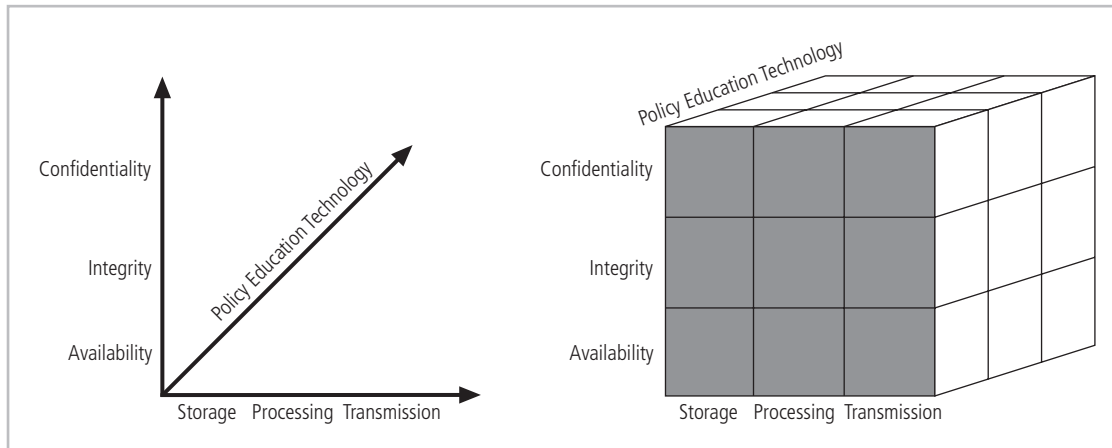


Figure 1-6 The McCumber Cube¹⁸

Source: *Course Technology/Cengage Learning*

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. The need for policy is discussed in subsequent chapters of this book.

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.

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.

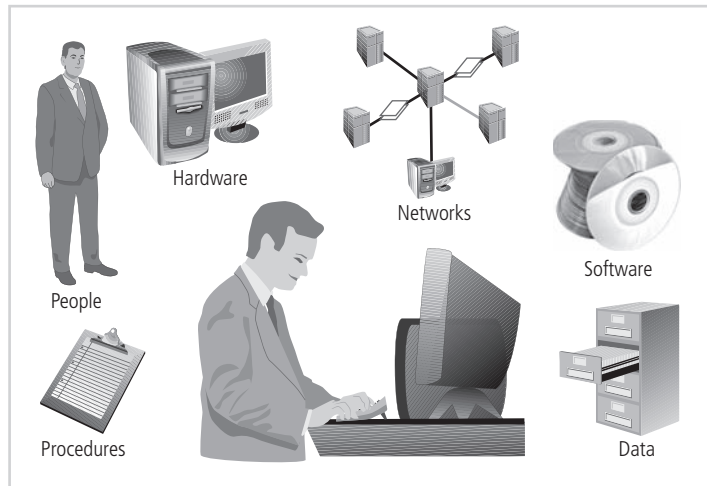


Figure 1-7 Components of an Information System

Source: Course Technology/Cengage Learning

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. This topic is discussed in more detail in Chapter 2, "The Need for Security."

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

security are essential, as is the implementation of alarm and intrusion systems to make system owners aware of ongoing compromises.



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.¹⁹

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

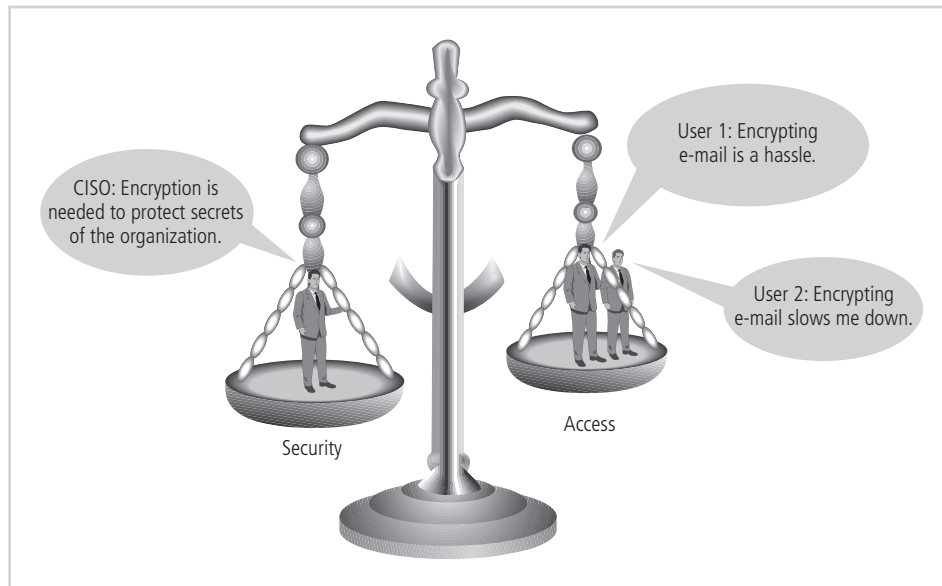


Figure 1-8 Balancing Information Security and Access

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.

Approaches to Information Security Implementation

The implementation of information security in an organization must begin somewhere, and cannot happen overnight. Securing information assets is in fact an incremental process that requires coordination, time, and patience. Information security can begin as a grassroots effort in which systems administrators attempt to improve the security of their systems. This is often referred to as a **bottom-up approach**. The key advantage of the bottom-up approach is the technical expertise of the individual administrators. Working with information systems on a day-to-day basis, these administrators possess in-depth knowledge that can greatly enhance the development of an information security system. They know and understand the threats to their systems and the mechanisms needed to protect them successfully. Unfortunately, this approach seldom works, as it lacks a number of critical features, such as participant support and organizational staying power.

The **top-down approach**—in which the project is initiated by upper-level managers who issue policy, procedures and processes, dictate the goals and expected outcomes, and determine accountability for each required action—has a higher probability of success. This approach has strong upper-management support, a dedicated champion, usually dedicated funding, a clear planning and implementation process, and the means of influencing organizational culture. The most successful kind of top-down approach also involves a formal development strategy referred to as a systems development life cycle.

For any organization-wide effort to succeed, management must buy into and fully support it. The role played in this effort by the champion cannot be overstated. Typically, this champion is an executive, such as a chief information officer (CIO) or the vice president of information technology (VP-IT), who moves the project forward, ensures that it is properly managed, and pushes for acceptance throughout the organization. Without this high-level support, many mid-level administrators fail to make time for the project or dismiss it as a low priority. Also critical to the success of this type of project is the involvement and support of the end users. These individuals are most directly affected by the process and outcome of the project and must be included in the information security process. Key end users should be assigned to a developmental team, known as the joint application development team (JAD). To succeed, the JAD must have staying power. It must be able to survive employee turnover and should not be vulnerable to changes in the personnel team that is developing the information security system. This means the processes and procedures must be documented and integrated into the organizational culture. They must be adopted *and promoted* by the organization's management.

The organizational hierarchy and the bottom-up and top-down approaches are illustrated in Figure 1-9.

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

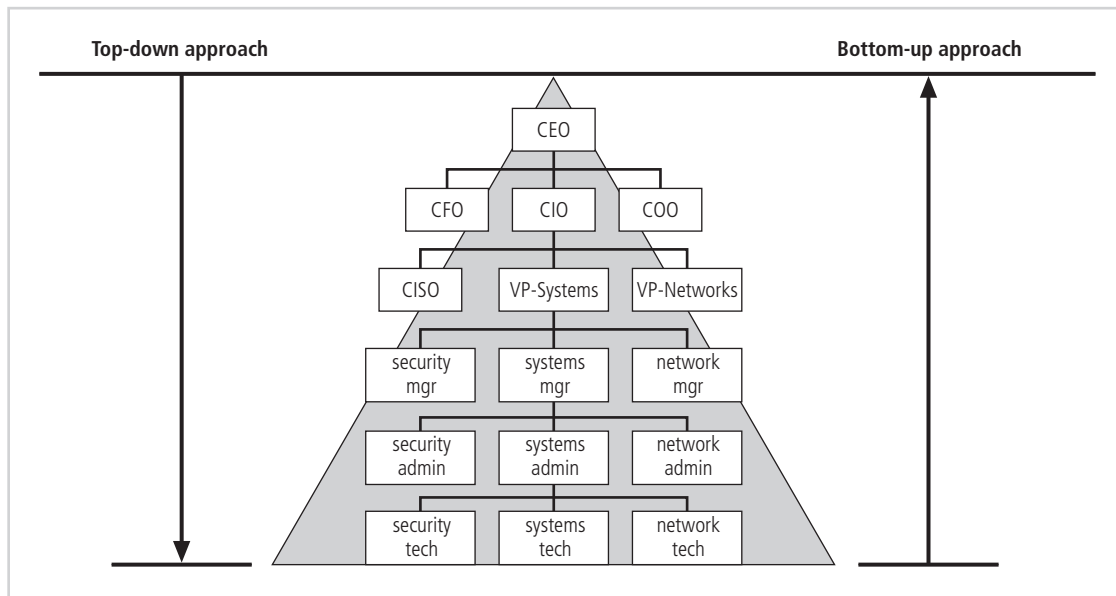


Figure 1-9 Approaches to Information Security Implementation

Source: Course Technology/Cengage Learning

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 can

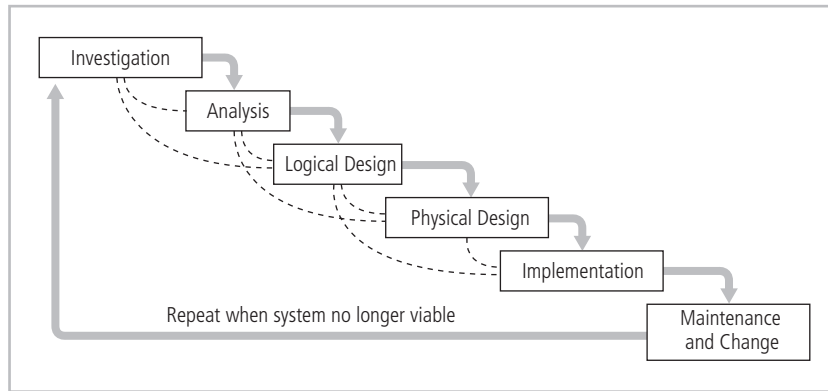


Figure 1-10 SDLC Waterfall Methodology

Source: Course Technology/Cengage Learning

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

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.*

Not For Sale

- *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.

The 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. This approach is discussed in subsequent chapters of this book.)

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. The EISP is covered in depth in Chapter 5 of this book.



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. Risk management is described in detail in Chapter 4 of this book.

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	<ul style="list-style-type: none"> Outline project scope and goals Estimate costs Evaluate existing resources Analyze feasibility 	<ul style="list-style-type: none"> Management defines project processes and goals and documents these in the program security policy
Phase 2: Analysis	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Analyze existing security policies and programs Analyze current threats and controls Examine legal issues Perform risk analysis
Phase 3: Logical Design	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Select technologies needed to support security blueprint Develop definition of successful solution Design physical security measures to support technological solutions Review and approve project
Phase 5: Implementation	<ul style="list-style-type: none"> Develop or buy software Order components Document the system Train users Update feasibility analysis Present system to users Test system and review performance 	<ul style="list-style-type: none"> Buy or develop security solutions At end of phase, present tested package to management for approval
Phase 6: Maintenance and Change	<ul style="list-style-type: none"> Support and modify system during its useful life Test periodically for compliance with business needs Upgrade and patch as necessary 	<ul style="list-style-type: none"> 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.



Security Professionals and the Organization

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.²²

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.

Communities of Interest

Each organization develops and maintains its own unique culture and values. Within each **organizational culture**, there are communities of interest that develop and evolve. As defined here, a **community of interest** is a group of individuals who are united by similar interests or values within an organization and who share a common goal of helping the organization to meet its objectives. While there can be many different communities of interest in an organization, this book identifies the three that are most common and that have roles and responsibilities in information security. In theory, each role must complement the other; in practice, this is often not the case.

Information Security Management and Professionals

The roles of information security professionals are aligned with the goals and mission of the information security community of interest. These job functions and organizational roles focus on protecting the organization's information systems and stored information from attacks.

Information Technology Management and Professionals

The community of interest made up of IT managers and skilled professionals in systems design, programming, networks, and other related disciplines has many of the same objectives as the information security community. However, its members focus more on costs of system creation and operation, ease of use for system users, and timeliness of system creation, as well as transaction response time. The goals of the IT community and the information security community are not always in complete alignment, and depending on the organizational structure, this may cause conflict.

Organizational Management and Professionals

The organization's general management team and the rest of the resources in the organization make up the other major community of interest. This large group is almost always made up of subsets of other interests as well, including executive management, production management, human resources, accounting, and legal, to name just a few. The IT community often categorizes these groups as users of information technology systems, while the information security community categorizes them as security subjects. In fact, this community serves as the greatest reminder that all IT systems and information security objectives exist to further the objectives of the broad organizational community. The most efficient IT systems operated in the most secure fashion ever devised have no value if they are not useful to the organization as a whole.

Information Security: Is it an Art or a Science?

Given the level of complexity in today's information systems, the implementation of information security has often been described as a combination of art and science. System technologists, especially those with a gift for managing and operating computers and computer-based systems, have long been suspected of using more than a little magic to keep the systems



Not For Sale

running and functioning as expected. In information security such technologists are sometimes called *security artisans*.²³ Everyone who has studied computer systems can appreciate the anxiety most people feel when faced with complex technology. Consider the inner workings of the computer: with the mind-boggling functions of the transistors in a CPU, the interaction of the various digital devices, and the memory storage units on the circuit boards, it's a miracle these things work at all.

Security as Art

The administrators and technicians who implement security can be compared to a painter applying oils to canvas. A touch of color here, a brush stroke there, just enough to represent the image the artist wants to convey without overwhelming the viewer, or in security terms, without overly restricting user access. There are no hard and fast rules regulating the installation of various security mechanisms, nor are there many universally accepted complete solutions. While there are many manuals to support individual systems, there is no manual for implementing security throughout an entire interconnected system. This is especially true given the complex levels of interaction among users, policy, and technology controls.

Security as Science

Technology developed by computer scientists and engineers—which is designed for rigorous performance levels—makes information security a science as well as an art. Most scientists agree that specific conditions cause virtually all actions in computer systems. Almost every fault, security hole, and systems malfunction is a result of the interaction of specific hardware and software. If the developers had sufficient time, they could resolve and eliminate these faults.

The faults that remain are usually the result of technology malfunctioning for any one of a thousand possible reasons. There are many sources of recognized and approved security methods and techniques that provide sound technical security advice. Best practices, standards of due care, and other tried-and-true methods can minimize the level of guesswork necessary to secure an organization's information and systems.

Security as a Social Science

A third view to consider is information security as a social science, which integrates some of the components of art and science and adds another dimension to the discussion. Social science examines the behavior of individuals as they interact with systems, whether these are societal systems or, as in this context, information systems. Information security begins and ends with the people inside the organization and the people that interact with the system, intentionally or otherwise. End users who need the very information the security personnel are trying to protect may be the weakest link in the security chain. By understanding some of the behavioral aspects of organizational science and change management, security administrators can greatly reduce the levels of risk caused by end users and create more acceptable and supportable security profiles. These measures, coupled with appropriate policy and training issues, can substantially improve the performance of end users and result in a more secure information system.

Selected Readings

- *Beyond Fear* by Bruce Schneier, 2006, Springer-Verlag, New York. This book is an excellent look at the broader areas of security. Of special note is Chapter 4, Systems and How They Fail, which describes how systems are often implemented and how they might be vulnerable to threats and attacks.
- *Fighting Computer Crime* by Donn B. Parker, 1983, Macmillan Library Reference.
- *Seizing the Enigma: The Race to Break the German U-Boats Codes, 1939–1943* by David Kahn, 1991, Houghton Mifflin.
- Glossary of Terms Used in Security and Intrusion Detection by SANS Institute. This can be accessed online at www.sans.org/resources/glossary.php.
- RFC 2828—Internet Security Glossary from the Internet RFC/STD/FYI/BCP Archives. This can be accessed online at www.faqs.org/rfcs/rfc2828.html.

Chapter Summary

- Information security evolved from the early field of computer security.
- Security is protection from danger. There are a number of types of security: physical security, personal security, operations security, communications security, national security, and network security, to name a few.
- Information security is the protection of information assets that use, store, or transmit information from risk through the application of policy, education, and technology.
- The critical characteristics of information, among them confidentiality, integrity, and availability (the C.I.A. triangle), must be protected at all times; this protection is implemented by multiple measures (policies, education training and awareness, and technology).
- Information systems are made up of six major components: hardware, software, data, people, procedures, and networks.
- Upper management drives the top-down approach to security implementation, in contrast with the bottom-up approach or grassroots effort, whereby individuals choose security implementation strategies.
- The traditional systems development life cycle (SDLC) is an approach to implementing a system in an organization and has been adapted to provide the outline of a security systems development life cycle (SecSDLC).
- The control and use of data in the organization is accomplished by
 - Data owners—responsible for the security and use of a particular set of information
 - Data custodians—responsible for the storage, maintenance, and protection of the information
 - Data users—work with the information to perform their daily jobs supporting the mission of the organization



- Each organization has a culture in which communities of interest are united by similar values and share common objectives. The three communities in information security are general management, IT management, and information security management.
- Information security has been described as both an art and a science, and also comprises many aspects of social science.

Review Questions

1. What is the difference between a threat agent and a threat?
2. What is the difference between vulnerability and exposure?
3. How is infrastructure protection (assuring the security of utility services) related to information security?
4. What type of security was dominant in the early years of computing?
5. What are the three components of the C.I.A. triangle? What are they used for?
6. If the C.I.A. triangle is incomplete, why is it so commonly used in security?
7. Describe the critical characteristics of information. How are they used in the study of computer security?
8. Identify the six components of an information system. Which are most directly affected by the study of computer security? Which are most commonly associated with its study?
9. What system is the father of almost all modern multiuser systems?
10. Which paper is the foundation of all subsequent studies of computer security?
11. Why is the top-down approach to information security superior to the bottom-up approach?
12. Why is a methodology important in the implementation of information security? How does a methodology improve the process?
13. Which members of an organization are involved in the security system development life cycle? Who leads the process?
14. How can the practice of information security be described as both an art and a science? How does security as a social science influence its practice?
15. Who is ultimately responsible for the security of information in the organization?
16. What is the relationship between the MULTICS project and the early development of computer security?
17. How has computer security evolved into modern information security?
18. What was important about Rand Report R-609?
19. Who decides how and when data in an organization will be used or controlled? Who is responsible for seeing that these wishes are carried out?
20. Who should lead a security team? Should the approach to security be more managerial or technical?



Exercises

1. Look up “the paper that started the study of computer security.” Prepare a summary of the key points. What in this paper specifically addresses security in areas previously unexamined?
2. 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 three components occupying that cell.
3. Consider the information stored on your personal computer. For each of the terms listed, find an example and document it: threat, threat agent, vulnerability, exposure, risk, attack, and exploit.
4. Using the Web, identify the chief information officer, chief information security officer, and systems administrator for your school. Which of these individuals represents the data owner? Data custodian?
5. Using the Web, find out more about Kevin Mitnick. What did he do? Who caught him? Write a short summary of his activities and explain why he is infamous.

Case Exercises

The next day at SLS found everyone in technical support busy restoring computer systems to their former state and installing new virus and worm control software. Amy found herself learning how to install desktop computer operating systems and applications as SLS made a heroic effort to recover from the attack of the previous day.

Questions:

1. Do you think this event was caused by an insider or outsider? Why do you think this?
2. Other than installing virus and worm control software, what can SLS do to prepare for the next incident?
3. Do you think this attack was the result of a virus or a worm? Why do you think this?

Endnotes

1. *Bletchley Park—Home of the Enigma machine*. Accessed 15 April 2010 from <http://churchwell.co.uk/bletchley-park-enigma.htm>.
2. Peter Salus. “Net Insecurity: Then and Now (1969–1998).” *Sane '98 Online*. 19 November 1998. Accessed 26 March 2007 from www.nluug.nl/events/sane98/after-math/salus.html.
3. Roberts, Larry. “Program Plan for the ARPANET.” Accessed 26 March 2007 from www.ziplink.net/~lroberts/SIGCOMM99_files/frame.htm.
4. Roberts, Larry. “Program Plan for the ARPANET.” Accessed 8 February 2007 from www.ziplink.net/~lroberts/SIGCOMM99_files/frame.htm.

5. Schell, Roger R., Downey, Peter J., and Popek, Gerald J. *Preliminary Notes on the Design of Secure Military Computer System*. January 1973. File, MCI-73-1, ESD/AFSC, Hanscom AFB, Bedford, MA 01731.
6. Bisbey, Richard, Jr., and Hollingsworth, Dennis. *Protection Analysis: Final Report*. May 1978. Final report, ISI/SR-78-13, USC/Information Sciences Institute, Marina Del Rey, CA 90291.
7. Grampp, F. T., and Morris, R. H. "UNIX Operating System Security." *AT&T Bell Laboratories Technical Journal* 63, no. 8 (1984): 1649–1672.
8. Peter Salus. "Net Insecurity: Then and Now (1969–1998)." *Sane '98 Online*. 19 November 1998. Accessed 26 March 2007 from www.nluug.nl/events/sane98/aftermath/salus.html.
9. Willis Ware. "Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security." *Rand Online*. 10 October 1979. Accessed 8 February 2007 from www.rand.org/pubs/reports/R609-1/R609.1.html.
10. Willis Ware. "Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security." *Rand Online*. 10 October 1979. Accessed 8 February 2004 from www.rand.org/publications/R/R609.1/R609.1.html.
11. Merriam-Webster. "security." *Merriam-Webster Online*. Accessed 8 February 2007 from www.m-w.com/dictionary/security.
12. National Security Telecommunications and Information Systems Security. *National Training Standard for Information Systems Security (Infosec) Professionals*. 20 June 1994. File, 4011. Accessed 8 Feb 2007 from www.cnss.gov/Assets/pdf/nstissi_4011.pdf.
13. Lemos, R. "HP's pretext to spy," *Security Focus Online*. Accessed 21 June 2007 from www.securityfocus.com/brief/296.
14. "ChoicePoint Data Theft Affected Thousands." *Wall Street Journal* (Eastern edition). 22 February 2005. New York, 1.
15. Dash, J. "ACLU Knocks Eli Lilly for Divulging E-Mail Addresses," *Computerworld* 35, no. 28 (9 July 2001): 6.
16. CyberCrime Staff. "FDA Flub." *G4*. Accessed 8 February 2007 from www.g4tv.com/techtvvault/features/39450/FDA_Flub.html.
17. Wikipedia. "The McCumber Cube." Accessed 16 February 2007 from http://en.wikipedia.org/wiki/McCumber_cube.
18. McCumber, John. "Information Systems Security: A Comprehensive Model." Proceedings of the 14th National Computer Security Conference, National Institute of Standards and Technology, Baltimore, MD, October 1991.
19. Microsoft. "C2 Evaluation and Certification for Windows NT (Q93362)." *Microsoft Online*. 1 November 2006. Accessed 25 January 2007 from <http://support.microsoft.com/default.aspx?scid=kb;en-us;93362>.
20. Adapted from Sandra D. Dewitz. *Systems Analysis and Design and the Transition to Objects*. 1996. New York: McGraw Hill Publishers, 94.

21. Grance, T., Hash, J., and Stevens, M. *Security Considerations in the Information System Development Life Cycle*. NIST Special Publication 800-64, rev. 1. Accessed 16 February 2007 from <http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf>.
22. Mary Hayes. "Where The Chief Security Officer Belongs." *InformationWeek* no. 877 (25 February 2002): 38.
23. D. B. Parker. *Fighting Computer Crime*. 1998. New York: Wiley Publishing, 189.



Not For Sale