

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 enough. 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 about four times an hour. 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 showed some of the facts: the user's name, his phone number and department, where his office was on the company campus, and a list of his past calls to the help desk.

"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?”

“Sure did. But the window wouldn’t close, and I had to turn my PC 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 help desk ticket status monitor on the wall at the end of the room. She saw that only two technicians were dispatched to user support at the moment, and since it was the day shift, four technicians were available. “Shouldn’t be long at all, Bob.”

She hung up and typed her notes into the company’s trouble ticket tracking system. She assigned the newly generated case to the user dispatch queue, which would page the roving user support technician with the details in 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 room where the company servers were kept in a carefully controlled environment. They all looked worried.

Just then, Amy’s screen beeped to alert her of a new e-mail. She glanced down. The screen beeped again—and again. It started beeping constantly. She clicked 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 in the Accounting Department. The subject line said, “Wait till you see this.” The message body read, “Funniest joke you’ll see today.” Davey often sent her interesting and funny e-mails, and she clicked the file attachment icon to open the latest joke.

After that click, 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 icon on her computer desktop to activate the call management software and activated her headset. “Hello, Help Desk, how can I help you?” She couldn’t greet the caller by name because her computer had not responded.

“Hello, this is Erin Williams in Receiving.”

Amy glanced down at her screen. Still no tracking system. 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 user support team either. She looked at the ticket status monitor again. It had gone dark. No numbers at all.

Then she saw Charlie running down the hall from the server room. His expression had changed from worried to 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
- Explain the role of security in the systems development life cycle
- Describe the information security roles of professionals within an organization

1

Introduction

Martin Fisher, IT Security Manager at Northside Hospital in Atlanta, believes that enterprise information security is a “critical business capability that needs to be aligned with corporate expectations and culture that provides the leadership and insight to identify risks and implement effective controls.” 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 information risks and controls may not be in balance at SLS. Though Amy works in a technical support role to help users with their problems, she did not recall her training about malicious e-mail attachments, such as worms or viruses, and fell victim to this form of attack herself. Understanding how malware might be the cause of a company’s problems is an important skill for information technology (IT) support staff as well as users. SLS’s 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 more capable of answering these questions. But, before you can begin studying details about the discipline of information security, you must first know its history and evolution.

The History of Information Security

Key Term

computer security In the early days of computers, this term specified the need to secure the physical location of computer technology from outside threats. This term later came to represent all actions taken to preserve computer systems from losses. It has evolved into the current concept of information security as the scope of protecting information in an organization has expanded.

The history of information security begins with the concept of **computer security**. The need for computer security arose during World War II when the first mainframe computers were developed and used to aid computations for communication code breaking messages from enemy



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: Bletchley Park Trust. Used with permission.²

cryptographic devices like the Enigma, shown in Figure 1-1. Multiple levels of security were implemented to protect these devices and the missions they served. This required new processes as well as tried-and-true methods needed to maintain data confidentiality. 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 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 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 a MOTD (message of the day) file while 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.³

› The 1960s

During the Cold War, many more mainframe computers were brought online to accomplish more complex and sophisticated tasks. These mainframes required a less cumbersome process of communication than mailing magnetic tapes between computer centers. In response to this need, the Department of Defense's Advanced Research Projects Agency (ARPA) began examining the feasibility of a redundant, networked communications system to support the military's exchange of information. In 1968, Dr. Larry Roberts developed the ARPANET

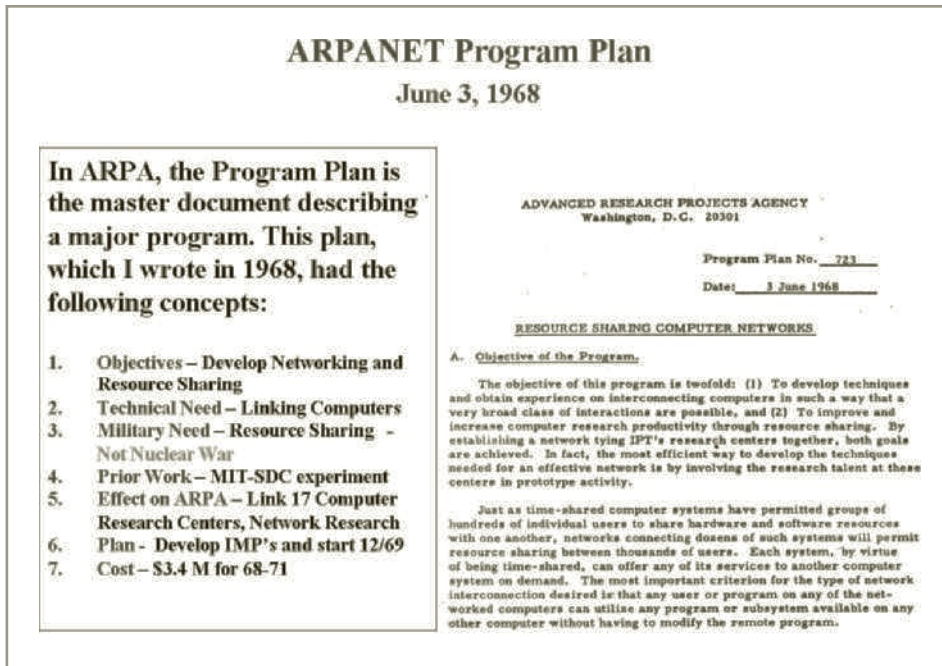


Figure 1-2 Development of the ARPANET

Source: Courtesy of Dr. Lawrence Roberts. Used with permission.⁴

project. Figure 1-2 is an excerpt from his Program Plan. ARPANET evolved into what we now know as the Internet, and Roberts became known as its founder.



For more information on Dr. Roberts and the history of the Internet, visit his Web site at www.packet.cc.

› The 1970s and 80s

During the next decade, ARPANET became more popular and saw wider use, increasing the potential for its misuse. In 1973, Internet pioneer Robert M. Metcalfe (pictured in Figure 1-3) identified fundamental problems with ARPANET security. As one of the creators of Ethernet, a dominant local area networking protocol, he knew that 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 authorizations. 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 commonly referred to as network insecurity.⁵ In 1978, Richard Bisbey and Dennis Hollingworth, two researchers in the Information Sciences Institute at the University of Southern California, published a study entitled “Protection Analysis: Final Report.” It focused on a project undertaken by ARPA to understand and detect vulnerabilities in



Figure 1-3 Dr. Metcalfe receiving the National Medal of Technology

Source: U.S. Department of Commerce. Used with permission.

operating system security. For a timeline that includes this and other seminal studies of computer security, see Table 1-1.

Security that went beyond protecting the physical location of computing devices effectively began with a single paper published by the RAND Corporation in February 1970 for the Department of Defense. RAND Report R-609 attempted to define the multiple controls and mechanisms necessary for the protection of a computerized data processing 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 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 both for the military and defense contractors.

In June 1967, ARPA formed a task force to study the process of securing classified information systems. The task force was assembled in October 1967 and met regularly to formulate recommendations, which ultimately became the contents of RAND Report R-609.⁶ The document was declassified in 1979 and released as Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security-RAND Report R-609-1. The content of the two documents is identical with the exception of two transmittal memorandums.



For more information on the RAND Report, visit www.rand.org/pubs/reports/R609-1.html.

Date	Document
1968	Maurice Wilkes discusses password security in <i>Time-Sharing Computer Systems</i> .
1970	Willis H. Ware authors the report <i>Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security-RAND Report R-609</i> , which was not declassified until 1979. It became known as the seminal work identifying the need for computer security.
1973	Schell, Downey, and Popek examine the need for additional security in military systems in <i>Preliminary Notes on the Design of Secure Military Computer Systems</i> .
1975	The Federal Information Processing Standards (FIPS) examines DES (Digital Encryption Standard) in the <i>Federal Register</i> .
1978	Bisbey and Hollingworth publish their study "Protection Analysis: Final Report," which discussed 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. ⁷
1979	Morris and Thompson author "Password Security: A Case History," published in the <i>Communications of the Association for Computing Machinery</i> (ACM). The paper examined the design history of 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," which discussed secure user IDs, secure group IDs, and the problems inherent in the systems.
1982	The U.S. Department of Defense Computer Security Evaluation Center publishes the first version of the Trusted Computer Security (TCSEC) documents, which came to be known as the Rainbow Series.
1984	Grampp and Morris write "The UNIX System: UNIX Operating System Security." In this report, the authors examined 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. ⁸
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 system administrator or other privileged users...the naive user has no chance." ⁹
1992	Researchers for the Internet Engineering Task Force, working at the Naval Research Laboratory, develop the Simple Internet Protocol Plus (SIPP) Security protocols, creating what is now known as IPSEC security.

Table 1-1 Key Dates in Information Security

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 use of networking components in military information systems introduced security risks that could not be mitigated by the routine practices then used to secure these systems. Figure 1-4 shows an illustration of computer network vulnerabilities from the 1979 release of this document. This paper signaled a pivotal moment in computer security history—the scope of computer security expanded significantly from the safety of physical locations and hardware to include:

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

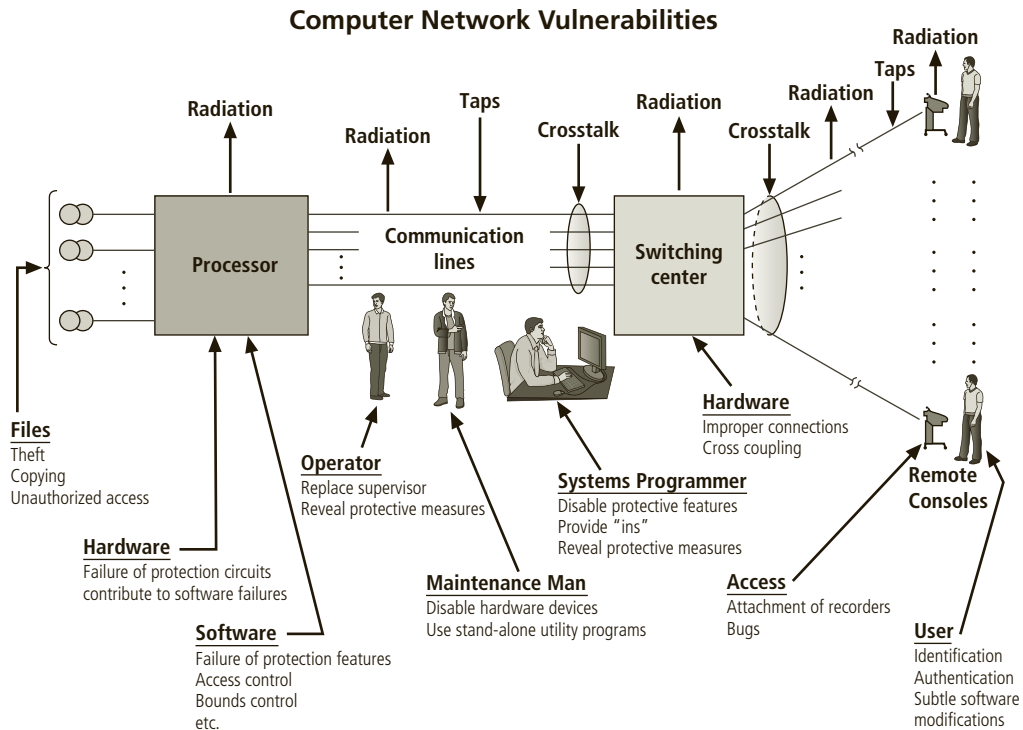


Figure 1-4 Illustration of computer network vulnerabilities from RAND Report R-609

Source: RAND Report R-609-1. Used with permission.¹⁰

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).



For more information on the MULTICS project, visit web.mit.edu/multics-history.

In 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. Not until the early 1970s did even the simplest component of security, the password function, become a component of UNIX.

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

In the early 1980s, TCP (the Transmission Control Protocol) and IP (the Internet Protocol) were developed and became the primary protocols for the ARPANET, eventually becoming the protocols we use on the Internet to this day. Also during this time frame, DNS, the hierarchical Domain Name System, was developed. The first dial-up Internet service provider (ISP)—The World, operated by Standard Tool & Die—came online, allowing home users to access the Internet. Prior to that, vendors like CompuServe, GENie, Prodigy, and Delphi had provided dial-up access for online computer services, while independent Bulletin Board Systems (BBSs) became popular for sharing information among their subscribers.



For more information on the history of the Internet, visit www.livescience.com/20727-internet-history.html.

In the mid-1980s, the U.S. Government passed several key pieces of legislation that formalized the recognition of computer security as a critical issue for federal information systems. The Computer Fraud and Abuse Act of 1986 and the Computer Security Act of 1987 defined computer security and specified responsibilities and associated penalties. These laws and others are covered in Chapter 3, “Legal, Ethical, and Professional Issues in Information Security.”

In 1988, the Defense Advanced Research Projects Agency (DARPA) within the Department of Defense created the Computer Emergency Response Team (CERT) to address network security.

› The 1990s

At the close of the 20th century, networks of computers became more common, as did the need to connect them 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 after decades of being 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 ARPANET, 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 interconnected networks did not exist. These de facto standards did little to ensure the security of information, though some degree of security was introduced as precursor technologies were widely adopted and became industry standards. However, early Internet deployment treated security as a low priority. In fact, many problems that plague e-mail on the Internet today result from 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.

In 1993, the first DEFCON conference was held in Las Vegas. Originally it was established as a gathering for people interested in information security, including authors, lawyers, government employees, and law enforcement officials. A compelling topic was the involvement of hackers in creating an interesting venue for the exchange of information between two adversarial groups—the “white hats” of law enforcement and security professionals and the “black hats” of hackers and computer criminals.

In the late 1990s and into the 2000s, many large corporations began publicly integrating security into their organizations. Antivirus products became extremely popular, and information security began to emerge as an independent discipline.

› 2000 to Present

Today, the Internet brings millions of unsecured computer networks and billions of computer systems into continuous communication with each other. The security of each computer's stored information is contingent on the security level 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 cyberattacks has made governments and companies more aware of the need to defend the computerized control systems of utilities and other critical infrastructure. Another growing concern is the threat of nation-states engaging in information warfare, and the possibility that business and personal information systems could become casualties if they are undefended. Since 2000, Sarbanes-Oxley and other laws related to privacy and corporate responsibility have affected computer security.

The attack on the World Trade Centers on September 11, 2001 resulted in major legislation changes related to computer security, specifically to facilitate law enforcement's ability to collect information about terrorism. The USA PATRIOT Act of 2001 and its follow-up laws, the USA PATRIOT Improvement and Reauthorization Act of 2005, the PATRIOT Sunsets Act of 2011, and the USA FREEDOM Act, are discussed in Chapter 3.



For more information on the history of computer security, visit the NIST Computer Security site at <http://csrc.nist.gov/publications/history/>. NIST is the National Institute of Standards and Technology.

What Is Security?

Key Terms

C.I.A. triad The industry standard for computer security since the development of the mainframe. The standard is based on three characteristics that describe the utility of information: confidentiality, integrity, and availability.

communications security The protection of all communications media, technology, and content.

information security Protection of the confidentiality, integrity, and availability of information assets, whether in storage, processing, or transmission, via the application of policy, education, training and awareness, and technology.

network security A subset of **communications security**; the protection of voice and data networking components, connections, and content.

security A state of being secure and free from danger or harm. Also, the actions taken to make someone or something secure.

Security is protection. Protection from adversaries—those who would do harm, intentionally or otherwise—is the ultimate objective of security. National security, for example, is a multi-layered 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 multiple layers of security in place to protect its operations, physical infrastructure, people, functions, communications, and information.

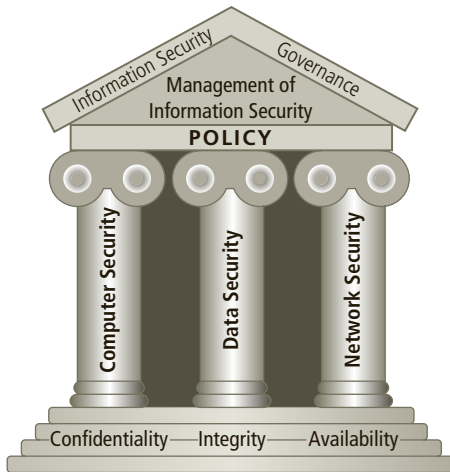


Figure 1-5 Components of information security

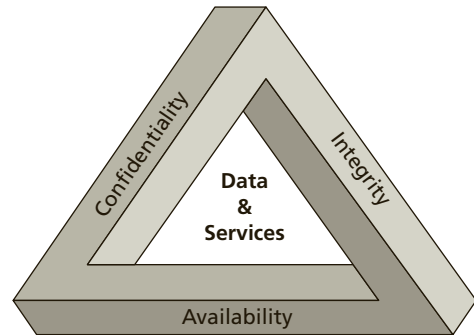


Figure 1-6 The C.I.A. triad

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 the information.¹¹ Figure 1-5 shows that information security includes the broad areas of information security management, 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. triad. The **C.I.A. triad** (see Figure 1-6) has been the standard for computer security in both industry and government since the development of the mainframe. This standard is based on the three characteristics of information that give it value to organizations: confidentiality, integrity, and availability. The security of these three characteristics is as important today as it has always been, but the C.I.A. triad model is generally viewed as no longer adequate in addressing 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 vast array of constantly evolving threats has prompted the development of a more robust model that addresses the complexities of the current information security environment. The expanded model consists of a list of critical characteristics of information, which are described in the next section. C.I.A. triad terminology is used in this chapter because of the breadth of material that is based on it.



For more information on CNSS, visit www.cnss.gov and click the About link, then select "History of CNSS."

➤ Key Information Security Concepts

This book uses many terms and concepts that are essential to any discussion of information security. Some of these terms are illustrated in Figure 1-7; all are covered in greater detail in subsequent chapters.

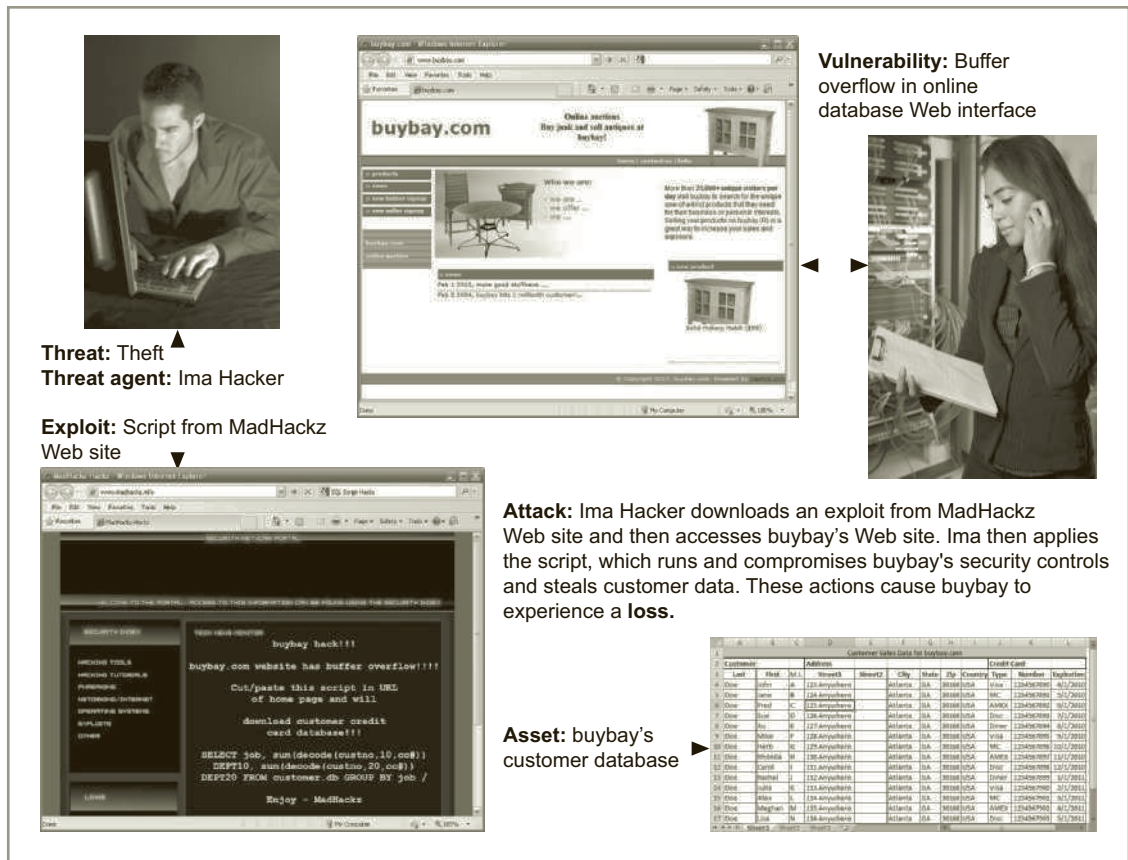


Figure 1-7 Key concepts in information security

Sources (top left to bottom right): © iStockphoto/tadija, Internet Explorer, © iStockphoto/darrenwise, Internet Explorer, Microsoft Excel.

- **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 must gain 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, software information, or data; or an asset can be physical, such as a person, computer system, hardware, or other tangible object. Assets, particularly information assets, are the focus of what security efforts are attempting to protect.
- **Attack:** An intentional or unintentional act that can damage or otherwise compromise information and the systems that support it. Attacks can be active or passive, intentional or unintentional, and direct or indirect. Someone who casually reads sensitive information not intended for his or her use is committing a passive attack. A hacker attempting to break into an information system is an intentional attack. A lightning strike that causes a building fire is an unintentional attack. A direct attack is perpetrated by a hacker using a PC to break into a system. An indirect attack is a hacker compromising a system and using it to attack other systems—for example, as part of a botnet (slang for *robot network*). This group of compromised computers, running

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

- **Control, safeguard, or countermeasure:** Security mechanisms, policies, or procedures that can successfully counter attacks, reduce risk, resolve vulnerabilities, and otherwise improve 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 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 is known to an attacker.
- **Loss:** A single instance of an information asset suffering damage or destruction, unintended or unauthorized modification or disclosure, or denial of use. 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 to protect the asset. The terms are sometimes used interchangeably with the term *security program*, although a security program often comprises managerial aspects of security, including planning, personnel, and subordinate programs.
- **Risk:** The probability of an unwanted occurrence, such as an adverse event or loss. Organizations must minimize risk to match their risk appetite—the quantity and nature of risk they are willing to accept.
- **Subjects and objects of attack:** 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 1-8. A computer can also be both the subject and object of an attack. For example, it can be compromised by an attack (object) and then used to attack other systems (subject).
- **Threat:** Any event or circumstance that has the potential to adversely affect operations and assets. The term *threat source* is commonly used interchangeably with the more generic term *threat*. While the two terms are technically distinct, in order to simplify discussion, the text will continue to use the term *threat* to describe threat sources.
- **Threat agent:** The specific instance or a component of a threat. For example, the threat source of “trespass or espionage” is a category of potential danger to information assets, while “external professional hacker” (like Kevin Mitnick, who was convicted of hacking into phone systems) is a specific threat agent. A lightning strike, hailstorm, or tornado is a threat agent that is part of the threat source known as “acts of God/acts of nature.”
- **Threat event:** An occurrence of an event caused by a threat agent. An example of a threat event might be damage caused by a storm. This term is commonly used interchangeably with the term *attack*.

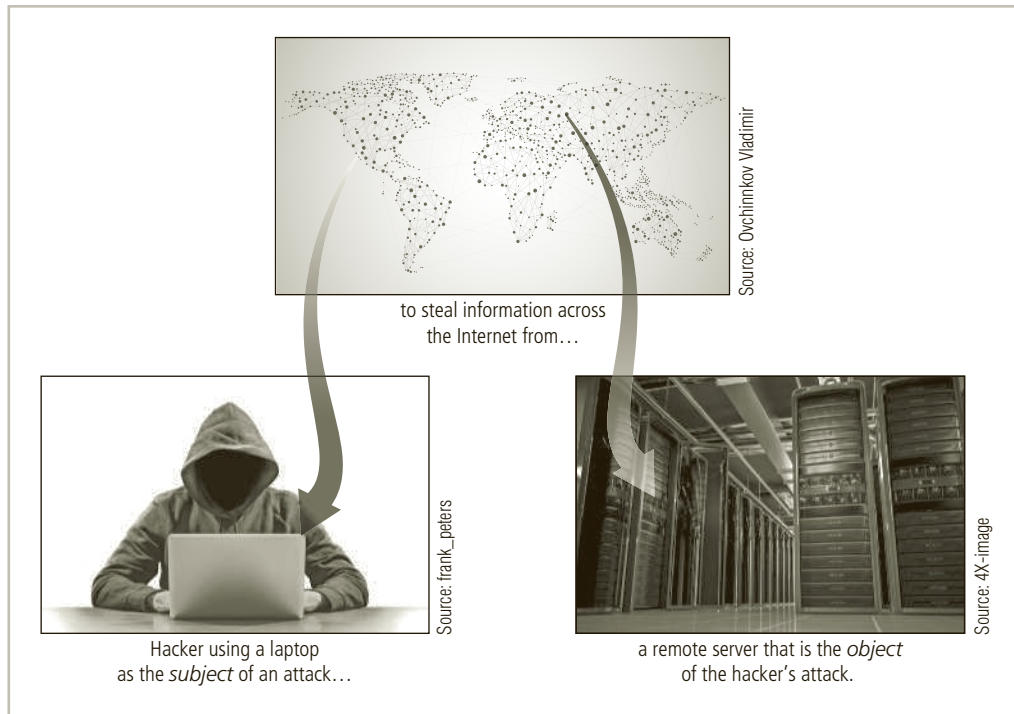


Figure 1-8 Computer as the subject and object of an attack

- **Threat source:** A category of objects, people, or other entities that represents the origin of danger to an asset—in other words, a category of threat agents. Threat sources are always present and can be purposeful or undirected. For example, threat agent “hackers,” as part of the threat source “acts of trespass or espionage,” purposely threaten unprotected information systems, while threat agent “severe storms,” as part of the threat source “acts of God/acts of nature,” incidentally threaten buildings and their contents.
- **Vulnerability:** A potential weakness in an asset or its defensive control system(s). 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

Key Terms

accuracy An attribute of information that describes how data is free of errors and has the value that the user expects.

authenticity An attribute of information that describes how data is genuine or original rather than reproduced or fabricated.

availability An attribute of information that describes how data is accessible and correctly formatted for use without interference or obstruction.

confidentiality An attribute of information that describes how data is protected from disclosure or exposure to unauthorized individuals or systems.

integrity An attribute of information that describes how data is whole, complete, and uncorrupted.

personally identifiable information (PII) A set of information that could uniquely identify an individual.

possession An attribute of information that describes how the data's ownership or control is legitimate or authorized.

utility An attribute of information that describes how data has value or usefulness for an end purpose.

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, depending on circumstances. For example, timeliness of information can be a critical factor because information loses much or all of its value when delivered too late. Though information security professionals and end users share an understanding of the characteristics of information, tensions can arise when the need to secure information from threats conflicts with the end users' need for unhindered access to it. For instance, end users may perceive a .1-second delay in the computation of data to be an unnecessary annoyance. Information security professionals, however, may perceive .1 seconds as a minor delay that enables an important task, like data encryption. Each critical characteristic of information—that is, the expanded C.I.A. triad—is defined in the following sections.

Availability Availability enables authorized users—people 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 the patron has free access to the book stacks. Once authorized patrons have access to the stacks, they expect to find the information they need in a usable format and familiar language. In this case, the information is bound in a book that is written in English.

Accuracy Information has accuracy when it is free from mistakes or errors and has the value that the end user expects. If information has been intentionally or unintentionally modified, it is no longer accurate. Consider a checking account, for example. You assume that the information in your account is an accurate representation of your finances. Incorrect information in the account can result from external or internal errors. If a bank teller, for instance, mistakenly adds or subtracts too much money 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 other 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 its origin. 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 the modified field often is the address of the originator. Spoofing the sender's address can fool e-mail recipients into thinking that the messages are legitimate traffic, thus inducing them to open e-mail they otherwise might not have.

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

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

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

The value of confidentiality is especially high for personal information about employees, customers, or patients. People 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, a healthcare facility, or a business. Problems arise when companies disclose confidential information. Sometimes this disclosure is intentional, but disclosure of confidential information also happens by mistake—for example, when confidential information is mistakenly e-mailed to someone *outside* the organization rather than to someone *inside* it.

Other examples of confidentiality breaches include 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 their clients, such as names, addresses, and credit card numbers.

As a consumer, you give up pieces of personal information in exchange for convenience or value almost daily. By using a “members” 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. When you sign up for a free magazine, Web resource, or free software application, you provide **personally identifiable information (PII)**. The bits and pieces of personal information you disclose may be copied, sold, replicated, distributed, and eventually coalesced into profiles and even complete dossiers of you and your life.

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

or other disruption of its authentic state. Corruption can occur while information is being 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 file size. Another key method of assuring information integrity is file hashing, in which a file is read by a special algorithm that uses the bit values in the file to compute a single large number called a hash value. The hash value for any combination of bits is unique.

OFFLINE

Unintentional Disclosures

The number of unintentional information releases due to malicious attacks is substantial. Millions of people lose information to hackers and malware-focused attacks annually. However, organizations occasionally lose, misplace, or inadvertently release information in an event not caused by hackers or other electronic attacks.

The Georgia Secretary of State gave out more than 6 million voters' private information, including Social Security numbers, in a breach that occurred in late 2015. The breach was found to have been caused by an employee who failed to follow established policies and procedures, and resulted in the employee being fired. While the agency claimed it recovered all copies of the data that were sent to 12 separate organizations, it was still considered a data breach.

In January 2008, GE Money, a division of General Electric, revealed that a data backup tape with credit card data from approximately 650,000 customers and over 150,000 Social Security numbers went missing from a records management company's storage facility. Approximately 230 retailers were affected when Iron Mountain, Inc., announced it couldn't find a magnetic tape.¹²

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, including names, addresses, and identification numbers. They did so without using any network or computer-based attacks; it was simple fraud. The fraud was feared to have allowed the perpetrators to arrange hundreds of identity thefts.

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 the mishap was caused by a programming error that occurred when patients who used a specific drug produced by Lilly signed up for an e-mail service to access company support materials.

If a computer system performs the same hashing algorithm on a file and obtains a different number than the file's recorded hash value, 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 hashing and hash values are examined in detail in Chapter 8, "Cryptography."



For more details on information losses caused by attacks, visit Wikipedia.org and search on the terms "Data breach" and "Timeline of Computer Security Hacker History."

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 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. In other words, information has value when it can serve a purpose. If information is available but is not in a meaningful format to the end user, it is not useful. For example, U.S. Census data can quickly become overwhelming and difficult for a private citizen to interpret; however, for a politician, the same data reveals information about 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 lead to 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 and 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 former employee nor anyone else can read it without the proper decryption methods; therefore, there is no breach of confidentiality. Today, people who are caught selling company secrets face increasingly stiff fines and a strong likelihood of jail time. Also, companies are growing more reluctant to hire people who have demonstrated dishonesty in their past. Another example might be that of a ransomware attack in which a hacker encrypts important information and offers to provide the decryption key for a fee. The attack would result in a breach of possession because the owner would no longer have possession of the information.

CNSS Security Model

Key Term

McCumber Cube A graphical representation of the architectural approach widely used in computer and information security; commonly shown as a cube composed of $3 \times 3 \times 3$ cells, similar to a Rubik's Cube.

The definition of information security in this text is based in part on the CNSS document called the National Training Standard for Information Systems Security Professionals, NSTISSI No. 4011 (1994). The hosting organization is the Committee on National Security Systems, which is responsible for coordinating the evaluation and publication of standards related to the protection of National Security Systems (NSS). CNSS was originally called the National Security Telecommunications and Information Systems Security Committee (NSTISSC) when established in 1990 by National Security Directive (NSD) 42, *National Policy for the Security of National Security Telecommunications and Information Systems*. The outdated CNSS standards are expected to be replaced by the newer NIST SP 800-16 Rev. 1 (2014), “A Role-Based Model for Federal Information Technology/Cyber Security Training,” in the near future.



For more information on CNSS and its standards, see www.cnss.gov/CNSS/issuances/Instructions.cfm.

The model, which was 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**.¹³ As shown in Figure 1-9, the McCumber Cube shows three dimensions. When 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 comprehensive system security, each of the 27 areas must be properly addressed during the security process. For example, the intersection of technology, integrity, and storage requires a set of controls or safeguards that address the need to use *technology* to protect the *integrity* of information while in *storage*. One such control might be a system for detecting host intrusion that protects the integrity of information by alerting security administrators to the potential modification of a critical file. A common omission from 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.

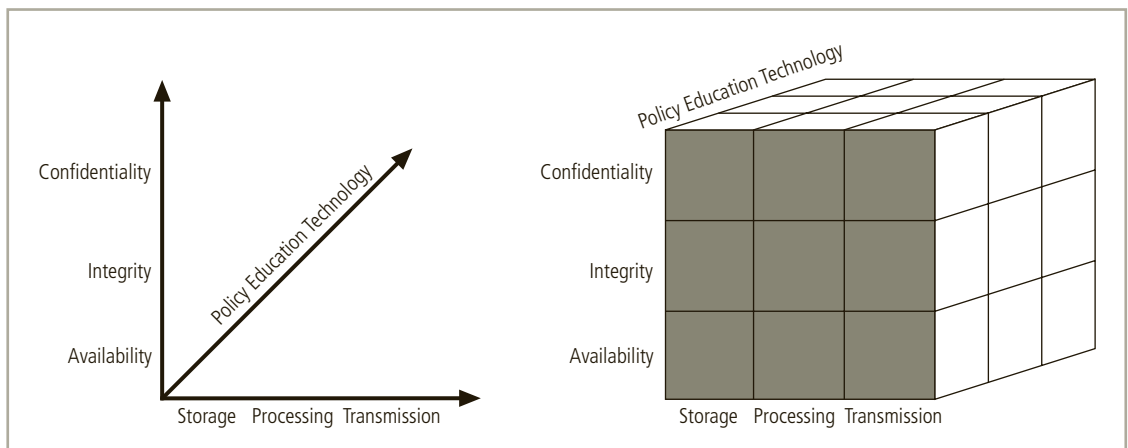


Figure 1-9 The McCumber Cube¹⁴

Components of an Information System

Key Terms

information system (IS) The entire set of software, hardware, data, people, procedures, and networks that enable the use of information resources in the organization.

physical security The protection of physical items, objects, or areas from unauthorized access and misuse.

As shown in Figure 1-10, an **information system (IS)** is much more than computer hardware; it is the entire set of people, procedures, and technology that enable business to use information. The six critical components of hardware, software, networks, people, procedures, and data 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 IS also has its own security requirements.

Software

The software component of an IS includes applications (programs), 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 (IT) 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.

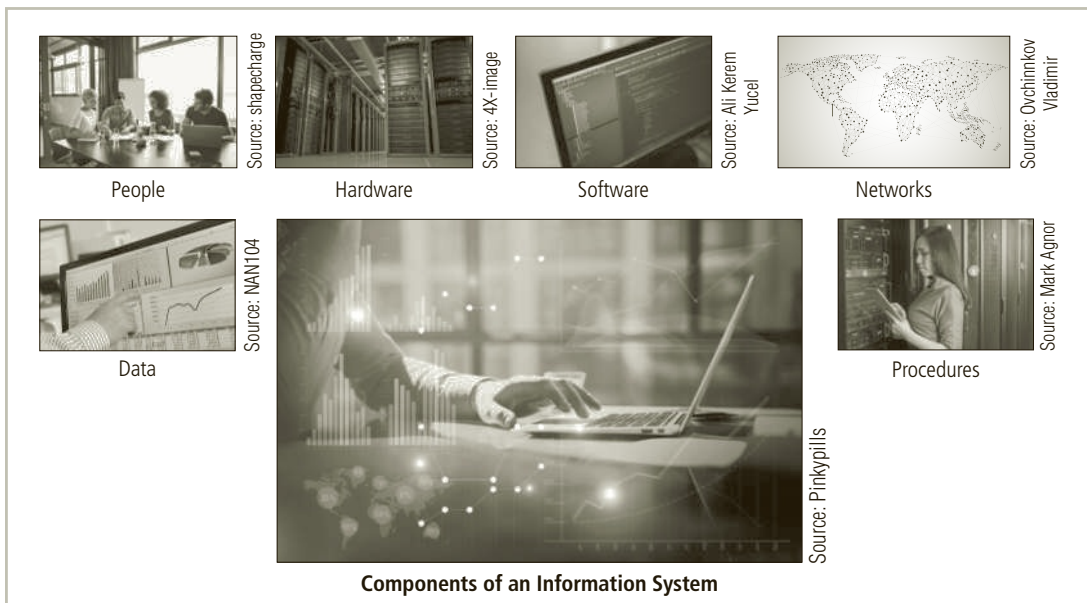


Figure 1-10 Components of an information system

Software carries the lifeblood of information through an organization. Unfortunately, software programs are often created under the constraints of project management, which limit time, costs, and manpower. Information security is all too often implemented as an afterthought rather than developed as an integral component from the beginning. In this way, software programs become an easy target of accidental or intentional attacks.

› Hardware

Hardware is the physical technology that houses and executes the software, stores and transports the data, and provides interfaces for the entry and removal of information from the system. **Physical security** policies deal with hardware as a physical asset and with the protection of physical assets from harm or theft. Applying the traditional tools of physical security, such as locks and keys, restricts access to and interaction with the hardware components of an information system. Securing the physical location of computers and the computers themselves is important because a breach of physical security can result in a loss of information. Unfortunately, most information systems are built on hardware platforms that cannot guarantee any level of information security if unrestricted hardware access 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 until the target placed the computer on the baggage scanner. As the computer was whisked through, the second perpetrator slipped ahead of the victim and entered the metal detector with a substantial collection of keys, coins, and the like, 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 did tighten the security process at airports, hardware can still be stolen in airports and other public places. Although laptops and notebook computers might be worth a few thousand dollars, the information stored on them can be worth a great deal more to disreputable organizations and individuals. Consider that unless plans and procedures are in place to quickly revoke privileges on stolen devices like laptops, tablets, and smartphones, the privileged access that these devices have to cloud-based data stores could be used to steal information that is many times more valuable than the device itself.

› Data

Data stored, processed, and transmitted by a computer system must be protected. Data is often the most valuable asset of an organization and therefore is the main target of intentional attacks. Systems developed in recent years are likely to make use of database management systems. When used properly, they should improve the security of the data and the applications that rely on the data. 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 make them less secure than traditional file systems. Because data and information exist in physical form in many organizations as paper reports, handwritten notes, and computer printouts, the protection of physical information is as important as the protection of electronic, computer-based information. As an aside, the terms *data* and *information* are used interchangeably today. Information was originally defined as *data with meaning*, such as a report or statistical

analysis. For our purposes, we will use the term *information* to represent both unprocessed data and actual information.

› 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 Hun invaders that the Chinese emperor commanded the construction of a great wall that would defend against them. Around 1275 A.D., Kublai Khan finally achieved what the Huns had been trying for more than a thousand 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. 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 people to obtain access information about a system. This topic is discussed in more detail in Chapter 2, "The Need for Security."

› Procedures

Procedures are another frequently overlooked component of an IS. Procedures are written instructions for accomplishing a specific task. When an unauthorized user obtains an organization's procedures, it 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), the bank consultant ordered millions of dollars to be transferred by wire to his own account. Lax security procedures caused the loss of more than \$10 million before the situation was corrected. Most organizations distribute procedures to employees so they can access the information system, but many of these companies often fail to provide proper education for using the procedures safely. 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 an organization on a need-to-know basis.

› Networks

Networking is the IS component that created much of the need for increased computer and information security. When information systems are connected to each other to form 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 accessible to organizations of every size. Applying the traditional tools of physical security, such as locks and keys, to restrict access to the system's hardware components is still important. However, when computer systems are networked, this approach is no longer enough. Steps to provide network security such as installing and configuring firewalls are essential,

as is implementing intrusion detection 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. Information security cannot be absolute: it is a process, not a goal. You can 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 only from the console in a secured room.¹⁵

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 1-11 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 obsessive focus on protecting and administering the information systems. Information security technologists and end users must recognize that both groups share the same overall goals of the organization—to ensure that data is available when, where, and how it is needed, with minimal delays or obstacles. In an ideal world, this level of availability can be met even after addressing concerns about loss, damage, interception, or destruction.

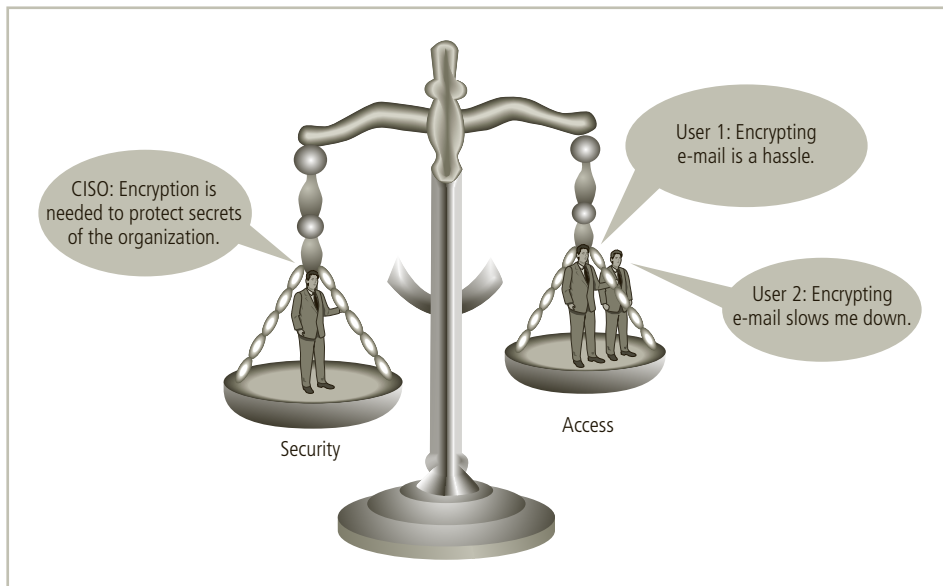


Figure 1-11 Balancing information security and access

Approaches to Information Security Implementation

Key Terms

bottom-up approach A method of establishing security policies and/or practices that begins as a grassroots effort in which systems administrators attempt to improve the security of their systems.

top-down approach A methodology of establishing security policies and/or practices that is initiated by upper management.

The implementation of information security in an organization must begin somewhere, and cannot happen overnight. Securing information assets is 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 individual administrators. By 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, the bottom-up approach seldom works because it lacks critical features such as participant support and organizational staying power.

The **top-down approach** has a higher probability of success. With this approach, the project is initiated by upper-level managers who issue policies, procedures, and processes; dictate the goals and expected outcomes; and determine accountability for each required action. 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 known as a systems development life cycle.

For any organization-wide effort to succeed, management must buy into and fully support it. The champion's role in this effort cannot be overstated. Typically, the 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. The involvement and support of end users is also critical to the success of this type of project. Users 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 (or design) 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 its relationship to the bottom-up and top-down approaches are illustrated in Figure 1-12.

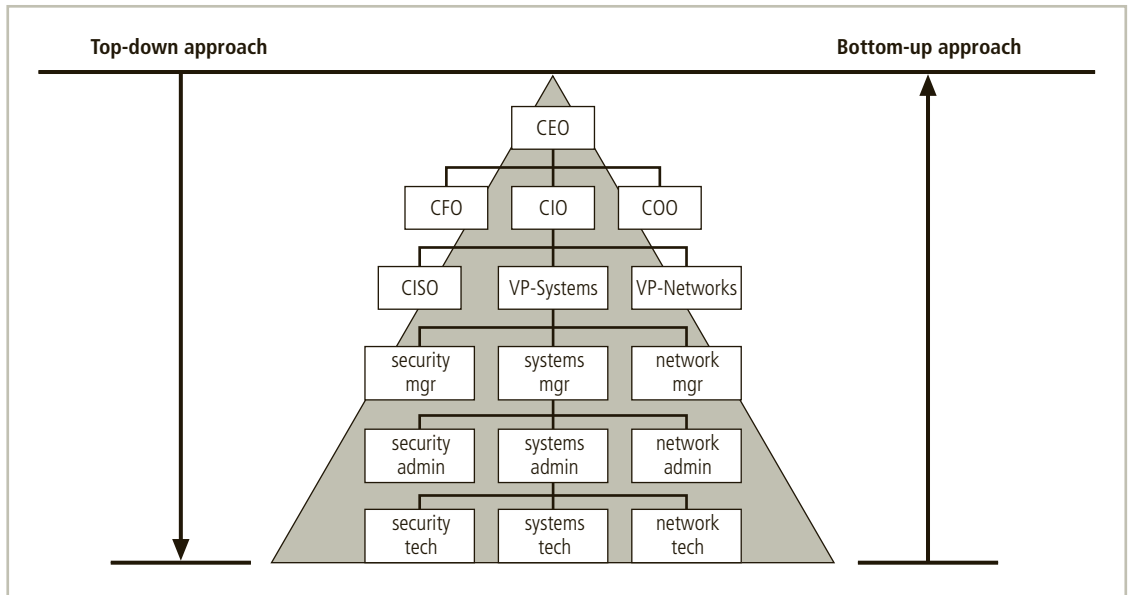


Figure 1-12 Approaches to information security implementation

Security in the Systems Development Life Cycle

Key Term

systems development life cycle (SDLC) A methodology for the design and implementation of an information system. The SDLC contains different phases depending on the methodology deployed, but generally the phases address the investigation, analysis, design, implementation, and maintenance of an information system.

Information security should be implemented into every major system in an organization. One approach for implementing information security into an organization's information systems is to ensure that security is a fundamental part of the organization's **systems development life cycle (SDLC)**. To understand how *security* is integrated into the systems development life cycle, you must first understand the foundations of systems development.

Each organization has a unique set of needs when it comes to how they might develop information (and security) systems. The organization's culture will dictate the nature and types of systems development activities that will be used. Many organizations do not develop a significant proprietary system, choosing instead to use off-the-shelf applications or work with other forms that specialize in the development and deployment of information systems. When organizations need to develop systems in-house, they can choose from a variety of approaches that have emerged over time. The traditional approach to software development (discussed in the next section) has given rise to a number of variations, including RAD, JAD, Agile, and one of the newest approaches, DevOps.

An early innovation in systems development was the inclusion of a broader cross-section of the organization in the development process. Whereas in early development projects, systems owners and software developers would collaborate to define specifications and create systems, an approach known as joint application development (JAD) added members of the management team from the supported business unit and in some cases, future users of the systems being created. Another innovation that often occurred with the JAD approach was to increase the speed at which requirements were collected and software was prototyped, thus allowing more iterations in the design process—an approach called rapid application development (RAD). This type of development later evolved into a combined approach known as the spiral method, in which each stage of development was completed in smaller increments, with delivery of working software components occurring more frequently and the software under development coming closer to its intended finished state with each pass through the development process.

Taking the objectives of JAD and RAD even further is the collective approach to systems development known as agile or extreme programming (XP), including aspects of systems development known as Kanban and scrum. As the need to reduce the time taken in the systems development cycle from gathering requirements to testing software continued to evolve, even faster feedback cycles were required to reduce time to market and shorten feature rollout times. When coupled with a need to better integrate the effort of the development team and the operations team to improve the functionality and security of applications, another model known as DevOps has begun to emerge.

DevOps focuses on integrating the need for the development team to provide iterative and rapid improvements to system functionality and the need for the operations team to improve security and minimize the disruption from software release cycles. By collaborating across the entire software/service lifecycle, DevOps uses a continuous development model that relies on systems thinking, short feedback loops, and continuous experimentation and learning.

Each of these approaches has its advantages and disadvantages, and each can be effective under the right circumstances. People who work in software development and some specialty areas of information security that support the software assurance process must be conversant with each of these methodologies.

An emerging development has been called SecOps by some. This is a process of using the DevOps methodologies of an integrated development and operations approach that is applied to the specification, creation, and implementation of security control systems.

› The Systems Development Life Cycle

Key Term

methodology A formal approach to solving a problem based on a structured sequence of procedures.

An SDLC is a **methodology** for the design and implementation of an information system. 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 is selected and made accountable for accomplishing the project goals.

› Traditional Development Methods

Key Term

waterfall model A type of SDLC in which each phase of the process “flows from” the information gained in the previous phase, with multiple opportunities to return to previous phases and make adjustments.

The traditional SDLC approach 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 three to twelve phases, all of which have been mapped into the six presented here. The **waterfall model** pictured in Figure 1-13 illustrates that each phase begins with the results and information gained from the previous phase.

At the end of each phase of the traditional SDLC 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. This determination depends on whether the project is proceeding as expected and whether it needs additional expertise, organizational knowledge, or other resources.

Once the system is implemented, it is maintained and modified over the remainder of its working life. Any information systems implementation may have multiple iterations as the cycle is repeated over time. Only by constant examination and renewal can any system, especially an information security program, perform up to expectations in a constantly changing environment.

The following sections describe each phase of a traditional SDLC.¹⁶

Investigation The first phase, investigation, is the most important. What problem is the system being developed to solve? The investigation phase begins by examining the

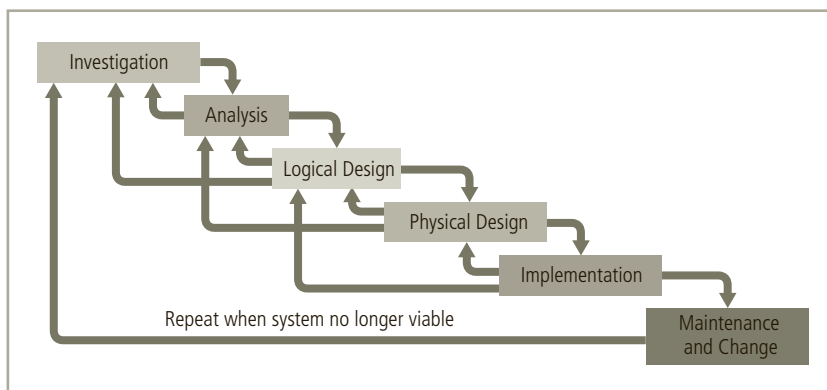


Figure 1-13 SDLC waterfall methodology

event or plan that initiates the process. During this phase, the objectives, constraints, and scope of the project are specified. A preliminary cost-benefit analysis evaluates the perceived benefits and their appropriate levels of cost. At the conclusion of this phase and at every phase afterward, a process will be undertaken to assess economic, technical, and behavioral feasibilities and ensure 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 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, the first and driving factor must be the business need. Based on the business need, applications are selected to provide needed services, and then the team chooses data support and structures capable of providing the needed inputs. Finally, based on all of this, specific technologies are delineated to implement the physical solution. The logical design, therefore, is the blueprint for the desired solution. The logical design is implementation independent, meaning that it contains no reference to specific technologies, vendors, or products. Instead, it addresses how the proposed system will solve the problem at hand. In this stage, analysts generate estimates of costs and benefits to allow 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—the option to develop 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 organization's 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. A feasibility analysis is again 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 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 the team determines 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. The people who manage and support the systems must continually monitor their effectiveness 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.



For more information on SDLCs, see Appendix E of NIST Special Publication 800-64, Rev. 2 at <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-64r2.pdf>.

› Software Assurance

Key Term

software assurance (SA) A methodological approach to the development of software that seeks to build security into the development life cycle rather than address it at later stages. SA attempts to intentionally create software free of vulnerabilities and provide effective, efficient software that users can deploy with confidence.

Many of the information security issues facing modern information systems have their root cause in the software elements of the system. Secure systems require secure or at least securable software. The development of systems and the software they use is often accomplished using a methodology, such as the SDLC described earlier. Many organizations recognize the need to include planning for security objectives in the SDLC they use to create systems, and have established procedures to create software that is more capable of being deployed in a secure fashion. This approach to software development is known as **software assurance**, or SA.

Organizations are increasingly working to build security into the SDLC to prevent security problems before they begin. A national effort is underway to create a common body of knowledge focused on secure software development. The U.S. Department of Defense launched a Software Assurance Initiative in 2003. This initial process was led by Joe Jarzombek and was endorsed and supported by the Department of Homeland Security (DHS), which joined the program in 2004. This program initiative resulted in the publication of the Secure Software Assurance (SwA) Common Body of Knowledge (CBK).¹⁷ A working group drawn from industry, government, and academia was formed to examine two key questions:

1. What are the engineering activities or aspects of activities that are relevant to achieving secure software?
2. What knowledge is needed to perform these activities or aspects?

Based on the findings of this working group and a host of existing external documents and standards, the SwA CBK was developed and published to serve as a guideline. While this work has not yet been adopted as a standard or even a policy requirement of

government agencies, it serves as a strongly recommended guide to developing more secure applications.

The SwA CBK, which is a work in progress, contains the following sections:

- Nature of Dangers
- Fundamental Concepts and Principles
- Ethics, Law, and Governance
- Secure Software Requirements
- Secure Software Design
- Secure Software Construction
- Secure Software Verification, Validation, and Evaluation
- Secure Software Tools and Methods
- Secure Software Processes
- Secure Software Project Management
- Acquisition of Secure Software
- Secure Software Sustainment¹⁸

The following sections provide insight into the stages that should be incorporated into the software SDLC.

➤ Software Design Principles

Good software development should result in a finished product that meets all of its design specifications. Information security considerations are a critical component of those specifications, though that has not always been true. Leaders in software development J. H. Saltzer and M. D. Schroeder note that:


*The protection of information in computer systems [... and] the usefulness of a set of protection mechanisms depends upon the ability of a system to prevent security violations. In practice, producing a system at any level of functionality that actually does prevent all such unauthorized acts has proved to be extremely difficult. Sophisticated users of most systems are aware of at least one way to crash the system, denying other users authorized access to stored information. Penetration exercises involving a large number of different general-purpose systems all have shown that users can construct programs that can obtain unauthorized access to information stored within. Even in systems designed and implemented with security as an important objective, design and implementation flaws provide paths that circumvent the intended access constraints. Design and construction techniques that systematically exclude flaws are the topic of much research activity, but no complete method applicable to the construction of large general-purpose systems exists yet...*¹⁹

This statement could be about software development in the early part of the 21st century, but it actually dates back to 1975, before information security and software assurance became

critical factors for many organizations. In the same article, the authors provide insight into what are now commonplace security principles:

- *Economy of mechanism: Keep the design as simple and small as possible.*
- *Fail-safe defaults: Base access decisions on permission rather than exclusion.*
- *Complete mediation: Every access to every object must be checked for authority.*
- *Open design: The design should not be secret, but rather depend on the possession of keys or passwords.*
- *Separation of privilege: Where feasible, a protection mechanism should require two keys to unlock, rather than one.*
- *Least privilege: Every program and every user of the system should operate using the least set of privileges necessary to complete the job.*
- *Least common mechanism: Minimize mechanisms (or shared variables) common to more than one user and depended on by all users.*
- *Psychological acceptability: It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly.*²⁰

Many of the common problems associated with programming approaches that don't follow the software assurance methodology are discussed in Chapter 2, "The Need for Security."



For more information on software assurance and the national effort to develop an SA common body of knowledge and supporting curriculum, visit <https://buildsecurityin.us-cert.gov/dhs/dhs-software-assurance-resources>.

› The NIST Approach to Securing the SDLC

NIST has adopted a simplified SLDC for their approach, based on five phases: initiation, development/acquisition, implementation/assessment, operation/maintenance, and disposal. These loosely map to the SDLC approach described earlier, as shown in Table 1-2.

Each phase of the SDLC should include consideration for the security of the system being assembled as well as the information it uses. Whether the system is custom-made and built

Waterfall SDLC Phase	Equivalent NIST SDLC Phase
Investigation	Initiation
Analysis	
Logical Design	Development/Acquisition
Physical Design	
Implementation	Implementation/Assessment
Maintenance and Change	Operation/Maintenance
	Disposal

Table 1-2 Comparison of Waterfall and NIST SDLC Phases

from scratch, purchased and then customized, or commercial off-the-shelf software (COTS), the implementing organization is responsible for ensuring its secure use. 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. 2, provides an overview of the security considerations for each phase of the SDLC.

While the following section offers advice from NIST expressed in the context of traditional methods (the waterfall methodology), note that these principles are equally valid when the effort uses RAD, JAD, Agile, XP, and other approaches to systems development. Development projects that make use of nontraditional development methodologies must still build in the requirements dictated by sound security practices. Software development should always include meeting security requirements.

To be most effective, information security must be integrated into the SDLC from system inception. Early integration of security in the SDLC enables agencies to maximize return on investment in their security programs, through:

- *Early identification and mitigation of security vulnerabilities and misconfigurations, resulting in lower cost of security control implementation and vulnerability mitigation;*
- *Awareness of potential engineering challenges caused by mandatory security controls;*
- *Identification of shared security services and reuse of security strategies and tools to reduce development cost and schedule while improving security posture through proven methods and techniques; and*
- *Facilitation of informed executive decision making through comprehensive risk management in a timely manner. [...]*

Initiation

During this first phase of the development life cycle, security considerations are key to diligent and early integration, thereby ensuring that threats, requirements, and potential constraints in functionality and integration are considered. At this point, security is looked at more in terms of business risks with input from the information security office. For example, an agency may identify a political risk resulting from a prominent Web site being modified or made unavailable during a critical business period, resulting in decreased trust by citizens.

Key security activities for this phase include:

- *Initial delineation of business requirements in terms of confidentiality, integrity, and availability;*
- *Determination of information categorization and identification of known special handling requirements to transmit, store, or create information such as personally identifiable information; and*
- *Determination of any privacy requirements.*

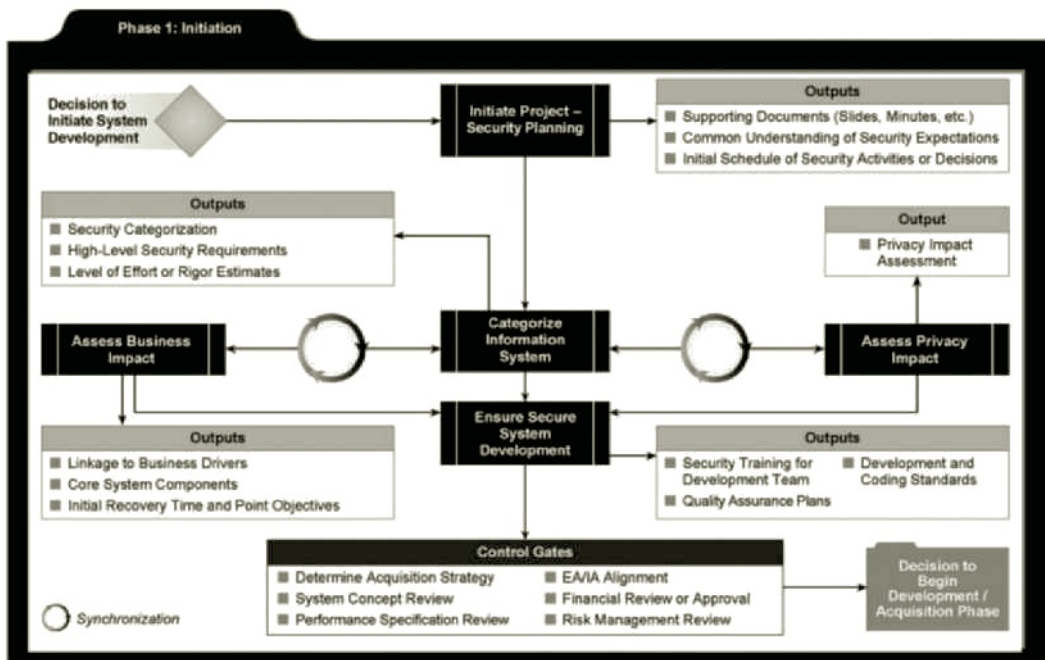


Figure 1-14 Relating security considerations in the Initiation phase

Source: NIST SP 800-64 Rev. 2: *Security Considerations in the System Development Life Cycle*.

Early planning and awareness will result in cost and time saving through proper risk management planning. Security discussions should be performed as part of (not separately from) the development project to ensure solid understandings among project personnel of business decisions and their risk implications to the overall development project. [...]

These activities and their related outputs are illustrated in Figure 1-14.

Development/Acquisition

This section addresses security considerations unique to the second SDLC phase.

Key security activities for this phase include:

- *Conduct the risk assessment and use the results to supplement the baseline security controls;*
- *Analyze security requirements;*
- *Perform functional and security testing;*
- *Prepare initial documents for system certification and accreditation; and*
- *Design security architecture.*

Although this section presents the information security components in a sequential top-down manner, the order of completion is not necessarily fixed. Security

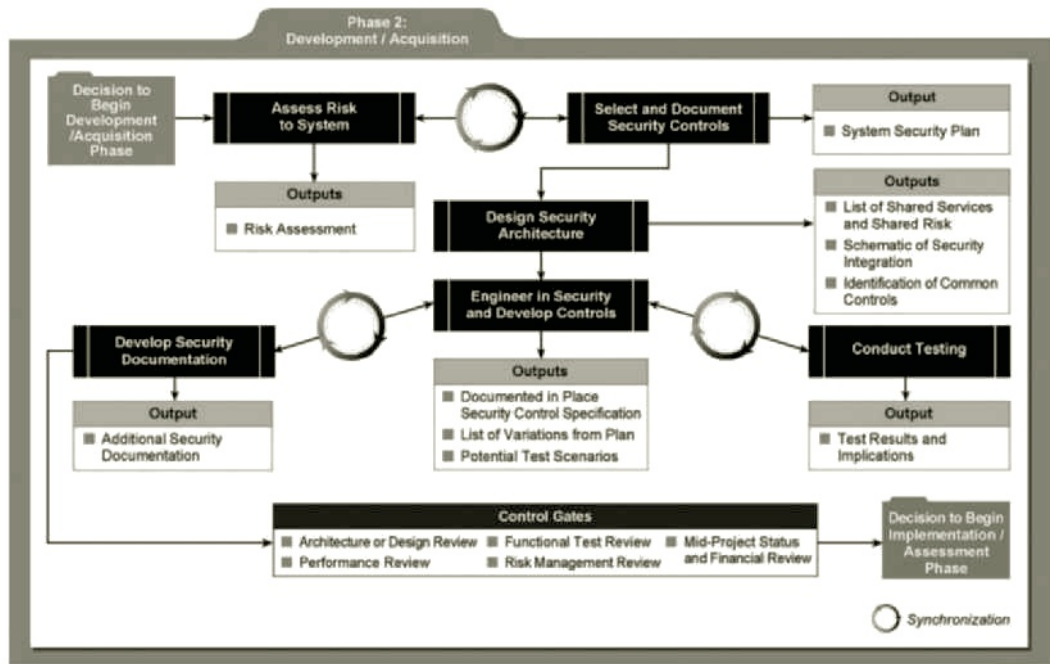


Figure 1-15 Relating security considerations in the Development/Acquisition phase

Source: NIST SP 800-64 Rev. 2: *Security Considerations in the System Development Life Cycle*.

analysis of complex systems will need to be iterated until consistency and completeness is achieved. [...]

These activities and their related outputs are illustrated in Figure 1-15.

Implementation/Assessment

Implementation/Assessment is the third phase of the SDLC. During this phase, the system will be installed and evaluated in the organization's operational environment.

Key security activities for this phase include:

- *Integrate the information system into its environment;*
- *Plan and conduct system certification activities in synchronization with testing of security controls; and*
- *Complete system accreditation activities. [...]*

Note that the Certification and Authorization (C&A) approach to systems formerly used by the federal government (discussed in later chapters in this text) has evolved into a comprehensive Risk Management Framework (RMF). As such, the performance of a risk assessment on the system under development would replace the C&A process. These activities and their related outputs are illustrated in Figure 1-16.

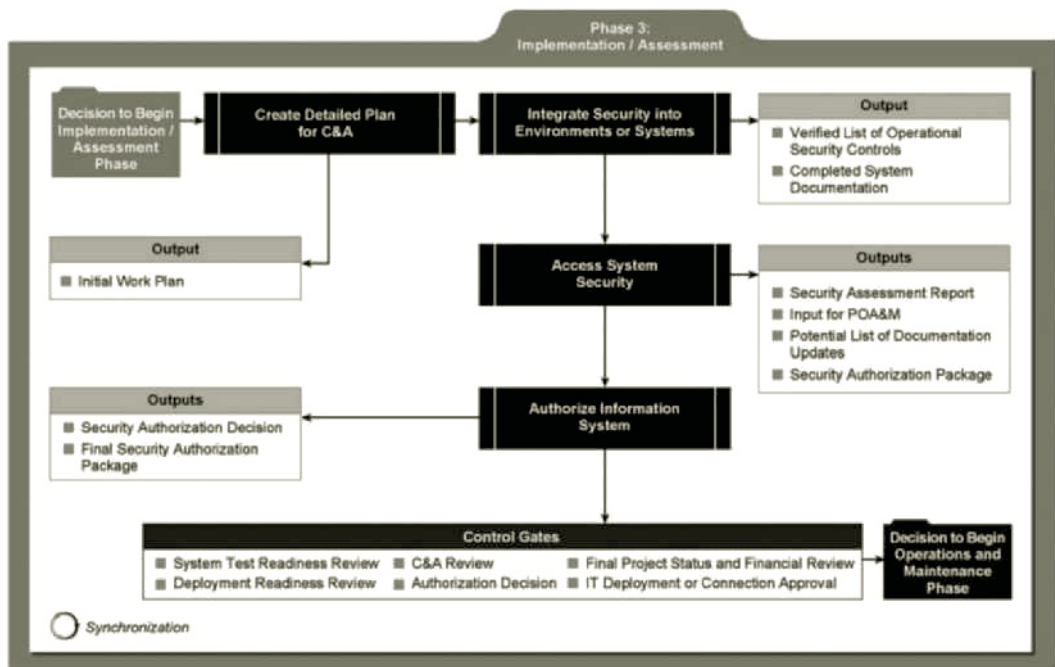


Figure 1-16 Relating security considerations in the Implementation/Assessment phase

Source: NIST SP 800-64 Rev. 2: Security Considerations in the System Development Life Cycle.

Operations and Maintenance

Operations and Maintenance is the fourth phase of the SDLC. In this phase, systems are in place and operating, enhancements and/or modifications to the system are developed and tested, and hardware and/or software is added or replaced. The system is monitored for continued performance in accordance with security requirements and needed system modifications are incorporated. The operational system is periodically assessed to determine how the system can be made more effective, secure, and efficient. Operations continue as long as the system can be effectively adapted to respond to an organization's needs while maintaining an agreed-upon risk level. When necessary modifications or changes are identified, the system may reenter a previous phase of the SDLC.

Key security activities for this phase include:

- Conduct an operational readiness review;
- Manage the configuration of the system;
- Institute processes and procedures for assured operations and continuous monitoring of the information system's security controls; and
- Perform reauthorization as required. [...]

These activities and their related outputs are illustrated in Figure 1-17.

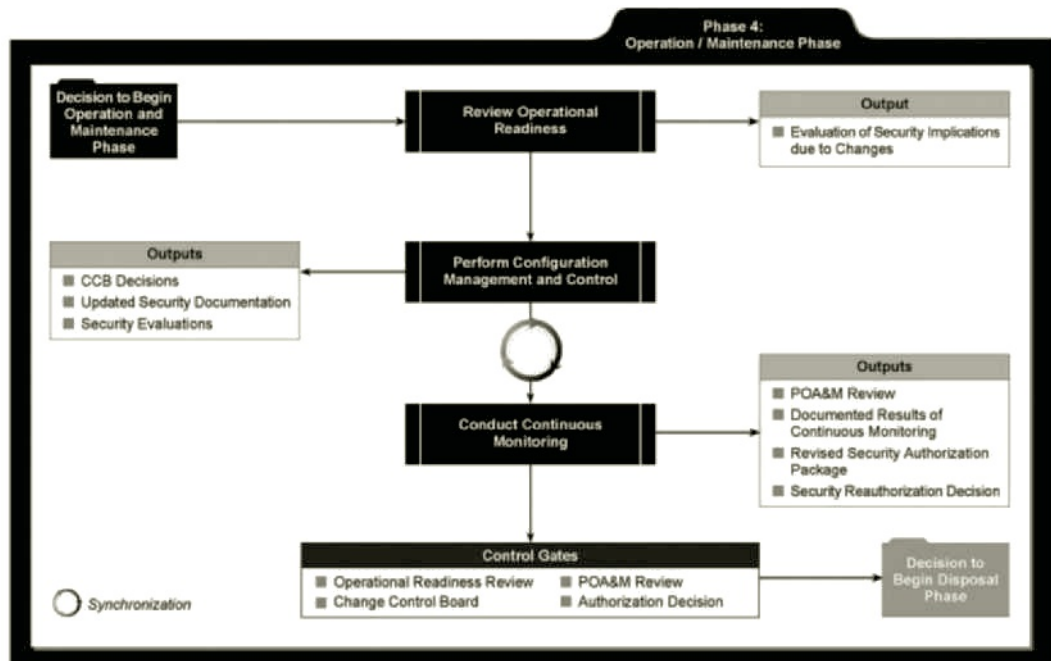


Figure 1-17 Relating security considerations in the Operation/Maintenance phase

Source: NIST SP 800-64 Rev. 2: Security Considerations in the System Development Life Cycle.

Disposal

Disposal, the final phase in the SDLC, provides for disposal of a system and closeout of any contracts in place. Information security issues associated with information and system disposal should be addressed explicitly. When information systems are transferred, become obsolete, or are no longer usable, it is important to ensure that government resources and assets are protected.

Usually, there is no definitive end to a system. Systems normally evolve or transition to the next generation because of changing requirements or improvements in technology. System security plans should continually evolve with the system. Much of the environmental, management, and operational information should still be relevant and useful in developing the security plan for the follow-on system.

The disposal activities ensure the orderly termination of the system and preserve the vital information about the system so that some or all of the information may be reactivated in the future, if necessary. Particular emphasis is given to proper preservation of the data processed by the system so that the data is effectively migrated to another system or archived in accordance with applicable records management regulations and policies for potential future access.

Key security activities for this phase include:

- Building and executing a disposal/transition plan;
- Archival of critical information;

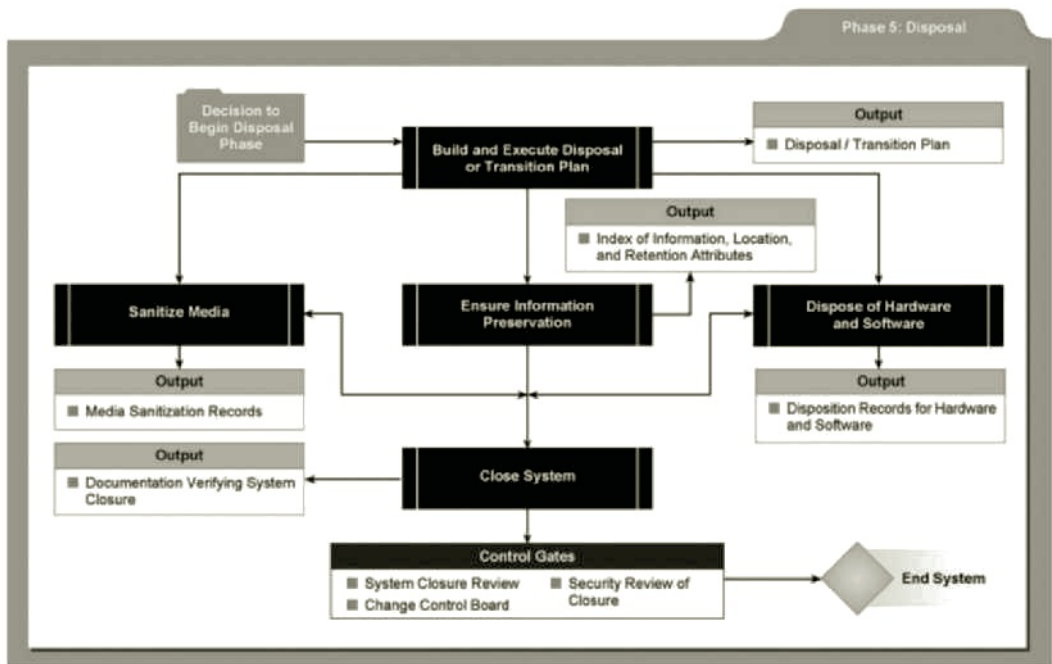


Figure 1-18 Relating security considerations in the Disposal phase

Source: NIST SP 800-64 Rev. 2: *Security Considerations in the System Development Life Cycle*.

- *Sanitization of media; and*
- *Disposal of hardware and software.*²¹

These activities and their related outputs are illustrated in Figure 1-18.

It is imperative that information security be designed into a system from its inception, rather than being added 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. A well-known adage holds 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 existing systems but consumer confidence in their products. In early 2002, Microsoft effectively suspended development work on many of its products to put its OS developers, testers, and program managers through an intensive program that focused 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. Since that time, Microsoft has developed its own Security Development Lifecycle, which uses a seven-phase, 16-step methodology that culminates in an executed incident response plan, as shown in Figure 1-19.



For more information on the Microsoft SDL, visit the Web site at www.microsoft.com/en-us/sdl.

Training	Requirements	Design	Implementation	Verification	Release	Response
1. Core security training	2. Establish security requirements	5. Establish design requirements	8. Use approved tools	11. Perform dynamic analysis	14. Create an incident response plan	Execute incident response plan
	3. Create quality gates/bug bars	6. Perform attack surface analysis/reduction	9. Deprecate unsafe functions	12. Perform fuzz testing	15. Conduct final security review	
	4. Perform security and privacy risk assessments	7. Use threat modeling	10. Perform static analysis	13. Conduct attack surface review	16. Certify release and archive	

Figure 1-19 Microsoft’s SDL²²

Source: Microsoft. Used with permission.

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. However, administrative support is also essential to developing and executing specific security policies and procedures, and of course technical expertise is essential to implementing the details of the information security program. The following sections describe typical information security responsibilities of various professional roles in an organization.

› Senior Management

Key Terms

chief information officer (CIO) An executive-level position that oversees the organization’s computing technology and strives to create efficiency in the processing and access of the organization’s information.

chief information security officer (CISO) Typically considered the top information security officer in an organization. The CISO is usually not an executive-level position, and frequently the person in this role reports to the CIO.

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 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.



Figure 1-20 The CISO's place and roles

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 by a similar title. The CISO usually reports directly to the CIO, although in larger organizations, one or more layers of management might 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 most common placement of CISOs in organizational hierarchies, along with their assigned roles and responsibilities, is illustrated in Figure 1-20. Note that such placement and accountabilities are the subject of current debate across the industry.²³

› Information Security Project Team

Key Term

project team A small functional team of people who are experienced in one or multiple facets of the required technical and nontechnical areas for the project to which they are assigned.

The information security **project team** should consist of people 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 also be a departmental line manager or staff unit manager, and 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 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 that do not disrupt the essential business activities they seek to safeguard.

› Data Responsibilities

Key Terms

data custodians Individuals who work directly with data owners and are responsible for storage, maintenance, and protection of information.

data owners Individuals who control, and are therefore responsible for, the security and use of a particular set of information; data owners may rely on custodians for the practical aspects of protecting their information, specifying which users are authorized to access it, but they are ultimately responsible for it.

data users Internal and external stakeholders (customers, suppliers, and employees) who interact with information in support of their organization's planning and operations.

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

- **Data owners:** Members of senior management who are responsible for the security and use of a particular set of information. 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 information and the systems that process, transmit, and store it. 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:** 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

Key Term

community of interest 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.

Each organization develops and maintains its own unique culture and values. Within each organizational culture, there are **communities of interest** that develop and evolve. While an organization can have many different communities of interest, 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, but this is often not the case in practice.

› 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 personnel 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 staff, 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 running as expected. In information security, such technologists are sometimes called *security artisans*.²⁴ 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 performed by the 1.4 billion transistors found in a CPU, the interaction of the various digital devices over the local networks and the Internet, and the memory storage units on the circuit boards, it's a miracle they 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 many manuals exist to support individual systems, no manual can help implement 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 all of these faults.

The faults that remain are usually the result of technology malfunctioning for any of a thousand 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 components of art and science and adds another dimension to the discussion. Social science examines the behavior of people as they interact with systems, whether they are societal systems or, as in this context, information systems. Information security begins and ends with the people inside the organization and the people who interact with the system, intentionally or otherwise.

What remains are those faults that are not really faults. There is a long-standing joke in IT that is sometimes told when a user has a system that is not performing as expected: “It’s not a bug, it’s a feature!” This situation occurs when a system performs as designed but not as expected, or when a user simply doesn’t have the skills to use the system effectively. The same is true when an attacker learns of unintended ways to use systems, not by taking advantage of defects in a system, but by taking advantage of unintended functions or operations. Although the science of the system may be exact, its use—the human side of systems—is not.

End users who need the very information that security personnel are trying to protect may be the weakest link in the security chain. By understanding some 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.