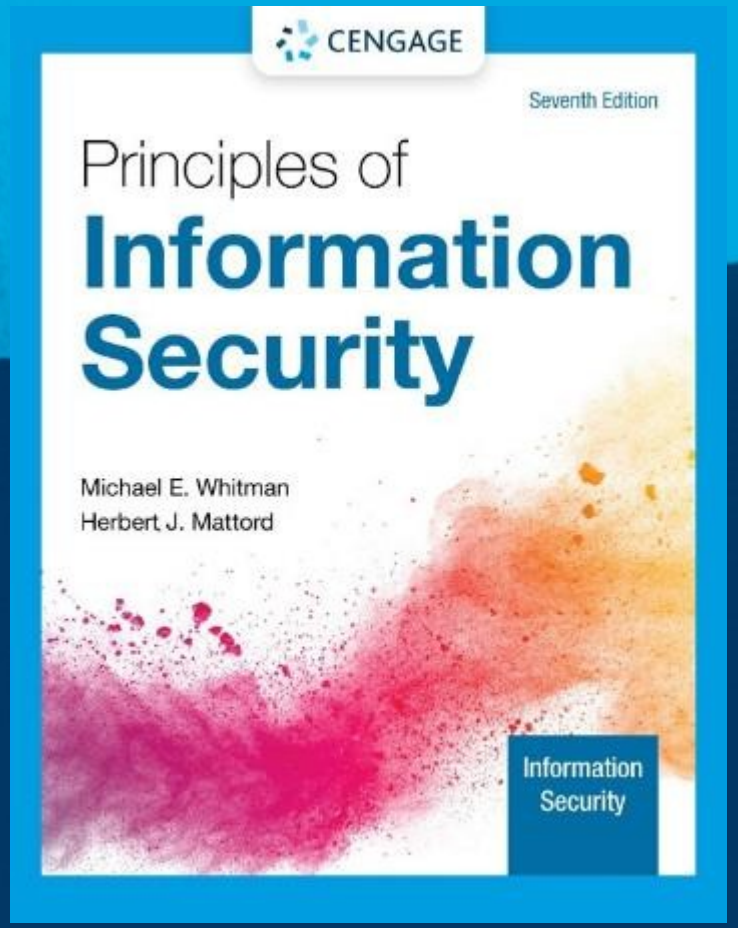


Module 1

Introduction to Information Security

Module Objectives

By the end of this module, you should be able to:

1.1 Define information security

1.2 Discuss the history of computer security and explain how it evolved into information security

1.3 Define key terms and critical concepts of information security

1.4 Describe the information security roles of professionals within an organization

Introduction

- Every organization, whether public or private and regardless of size, has information it wants to protect.
- Organizations have a responsibility to all their stakeholders to protect that information.
- Unfortunately, there aren't enough security professionals to go around.
- If you're not part of the solution, you're part of the problem.

The History of Information Security

- Computer security began immediately after the first mainframes were developed.
  - Groups developing code-breaking computations during World War II created the first modern computers.
  - Multiple levels of security were implemented to protect these devices.
- 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.

The Enigma

© kamilpetran/Shutterstock.com

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."

Source: © kamilpetran/Shutterstock.com.

Figure 1-1 The Enigma

Key Dates in Information Security (1 of 3)

Date	Document
1968	Maurice Wilkes discusses password security in *Time-Sharing Computer Systems*.
1970	Willis H. Ware authors the report "Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security-RAND Report R-609," 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 *Preliminary Notes on the Design of Secure Military Computer Systems*.
1975	The Federal Information Processing Standards (FIPS) examines DES (Digital Encryption Standard) in the *Federal Register*.
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.

Key Dates in Information Security (2 of 3)

Date	Document
1979	Morris and Thompson author “Password Security: A Case History," published in the *Communications of the Association for Computing Machinery* (ACM). The paper examined the design history of a password security scheme on a remotely accessed, time-sharing system. 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.

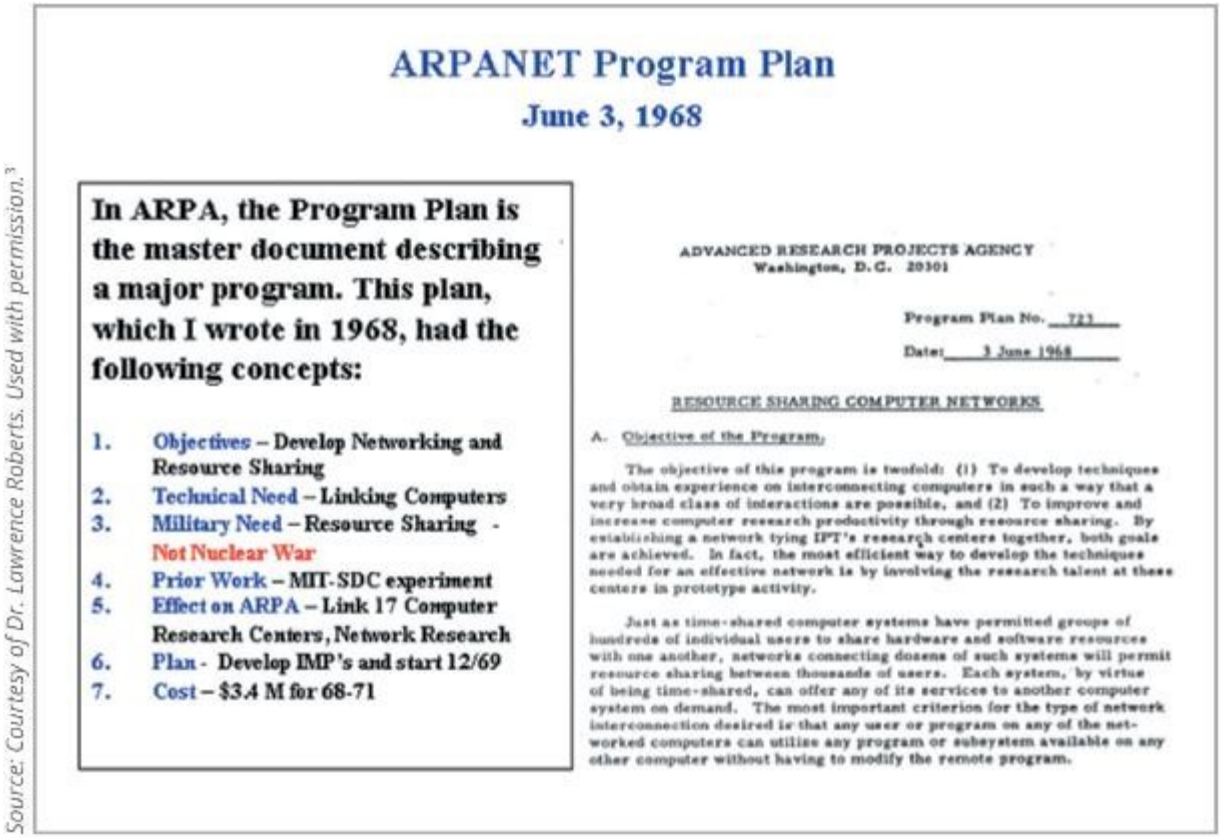
Key Dates in Information Security (3 of 3)

Date	Document
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. 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.“
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.

The 1960s

- During the Cold War, many more mainframe computers were brought online to accomplish more complex and sophisticated tasks.
- The Advanced Research Projects Agency (ARPA) began to examine the feasibility of a redundant networked communication system.
- Larry Roberts led the development of the ARPANET, which evolved into what we now know as the Internet.

Development of the ARPANET



Source: Courtesy of Dr. Lawrence Roberts. Used with permission.[3]

Figure 1-2 Development of the ARPANET

The 1970s and ’80s (1 of 2)

- ARPANET grew in popularity, increasing the potential for misuse.
- Fundamental problems with ARPANET security were identified.
  - Individual remote sites did not have sufficient controls and safeguards to protect data from unauthorized remote users.
  - Other problems included:
    - Vulnerability of password structure and formats
    - Lack of safety procedures for dial-up connections
    - Nonexistent user identification and authorizations

The 1970s and ’80s (2 of 2)

- Information security began with RAND Report R-609—the paper that started the study of computer security and identified the role of management and policy issues in it.
- The scope of computer security grew from physical security to include:
  - Securing the data
  - Limiting random and unauthorized access to data
  - Involving personnel from multiple levels of the organization in information security

Computer Network Vulnerabilities

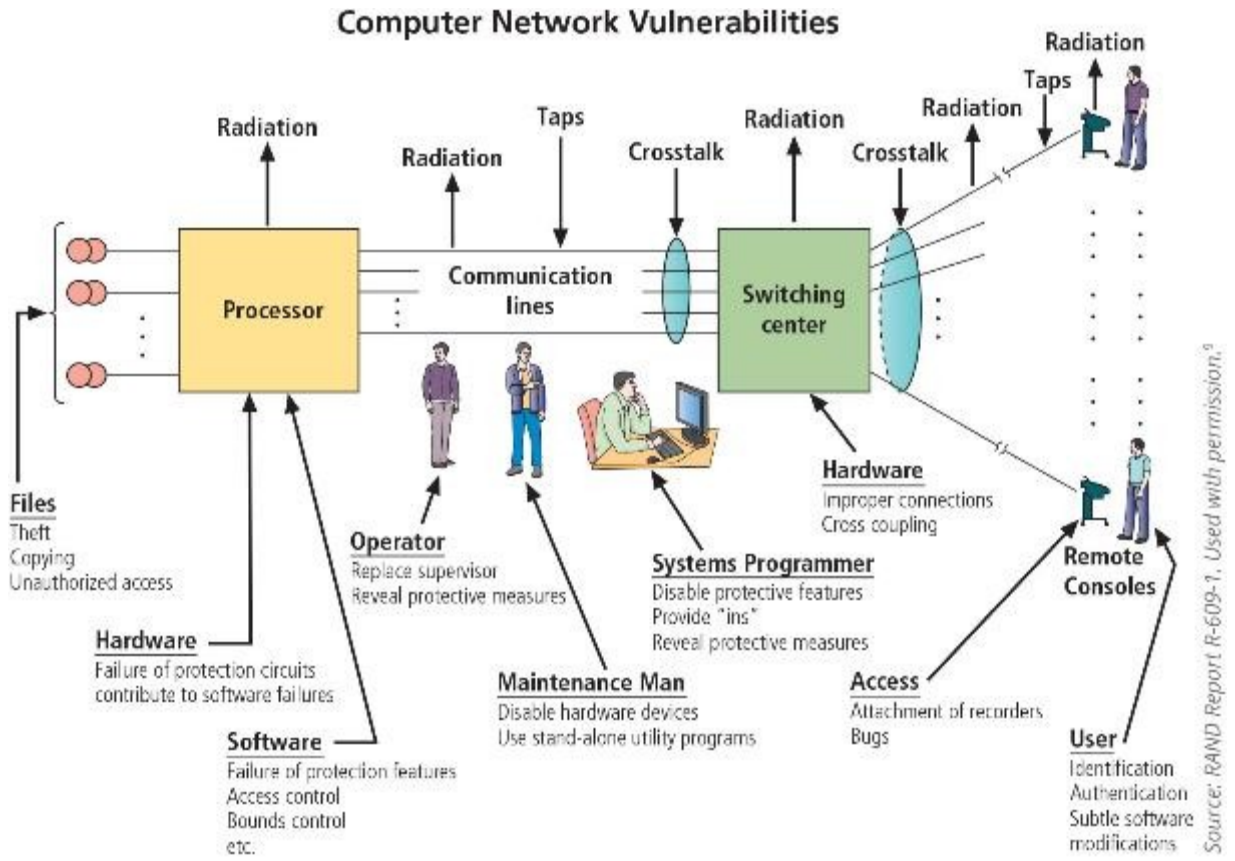


Figure 1-4 Illustration of computer network vulnerabilities from RAND Report R-609

MULTICS

- Early research on computer security research centered on a system called Multiplexed Information and Computing Service (MULTICS).
- The first operating system was created with security integrated into core functions.
- Mainframe, time-sharing OS was developed in the mid-1960s by General Electric (GE), Bell Labs, and Massachusetts Institute of Technology (MIT).
- Several MULTICS key players created UNIX.
  - The primary purpose of UNIX was text processing.
- Late 1970s: The microprocessor expanded computing capabilities and security threats.

The 1990s

- Networks of computers became more common, as did the need to connect them to each other.
- The Internet became the first global network of networks.
- Initially, network connections were based on de facto standards.
- In early Internet deployments, security was treated as a low priority.
- In the late 1990s and into the 2000s, many large corporations began publicly integrating security into their organizations.

Information security began to emerge as an independent discipline.

2000 to Present

- The Internet brings millions of unsecured computer networks and billions of computer systems into continuous communication with each other.
- The ability to secure a computer's data was influenced by the security of every computer to which it is connected.
- The growing threat of cyberattacks has increased the awareness of need for improved security.
- The threat environment has grown from the semiprofessional hacker defacing Web sites for amusement to professional cybercriminals maximizing revenue from theft and extortion, as well as government-sponsored cyberwarfare groups striking military, government, and commercial targets.

What Is Security?

- "A state of being secure and free from danger or harm; the actions taken to make someone or something secure."
- "The protection of information and its critical elements, including systems and hardware that use, store, and transmit that information" (CNSS).
- InfoSec Includes information security management, data security, and network security.
- C.I.A. triad of confidentiality, integrity, and availability:
  - Is a standard based on confidentiality, integrity, and availability, now viewed as inadequate.
  - Expanded model consists of a list of critical characteristics of information

Knowledge Check Activity 1

What is security?

a. Freedom from fear
b. Protection from loss
c. Keeping secrets
d. Being secure and free from danger

Knowledge Check Activity 1: Answer

What is security?

Answer: D. Being secure and free from danger

Only this answer is complete. Fear has little to do with security; many are fearful even when secure. Security does not mean losses cannot occur, just that they are planned for and survivable. Confidentiality (secrets) is just one of the three key aspects of security.

Components of Information Security

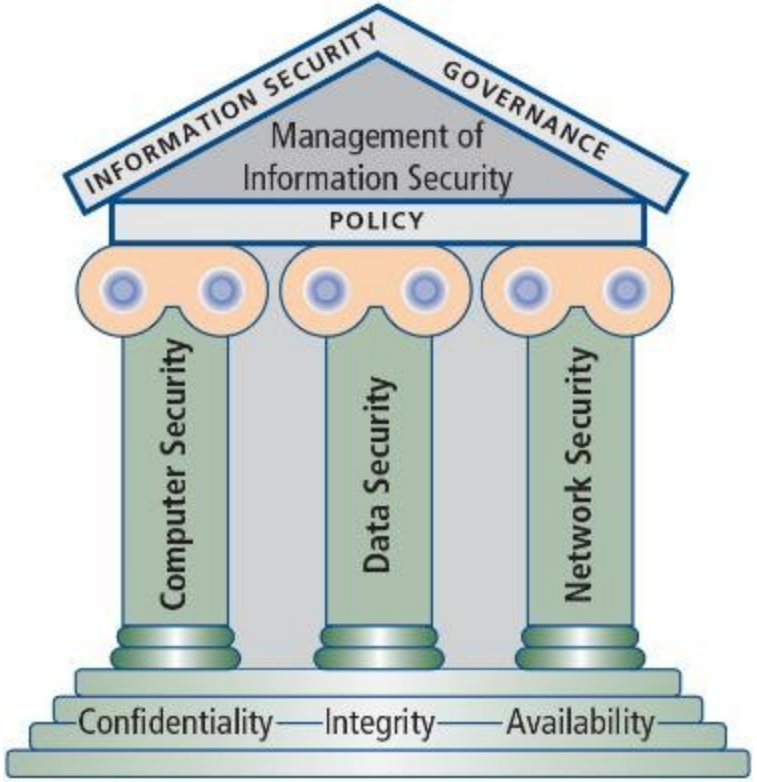


Figure 1-5 Components of information security

The C.I.A. Triad

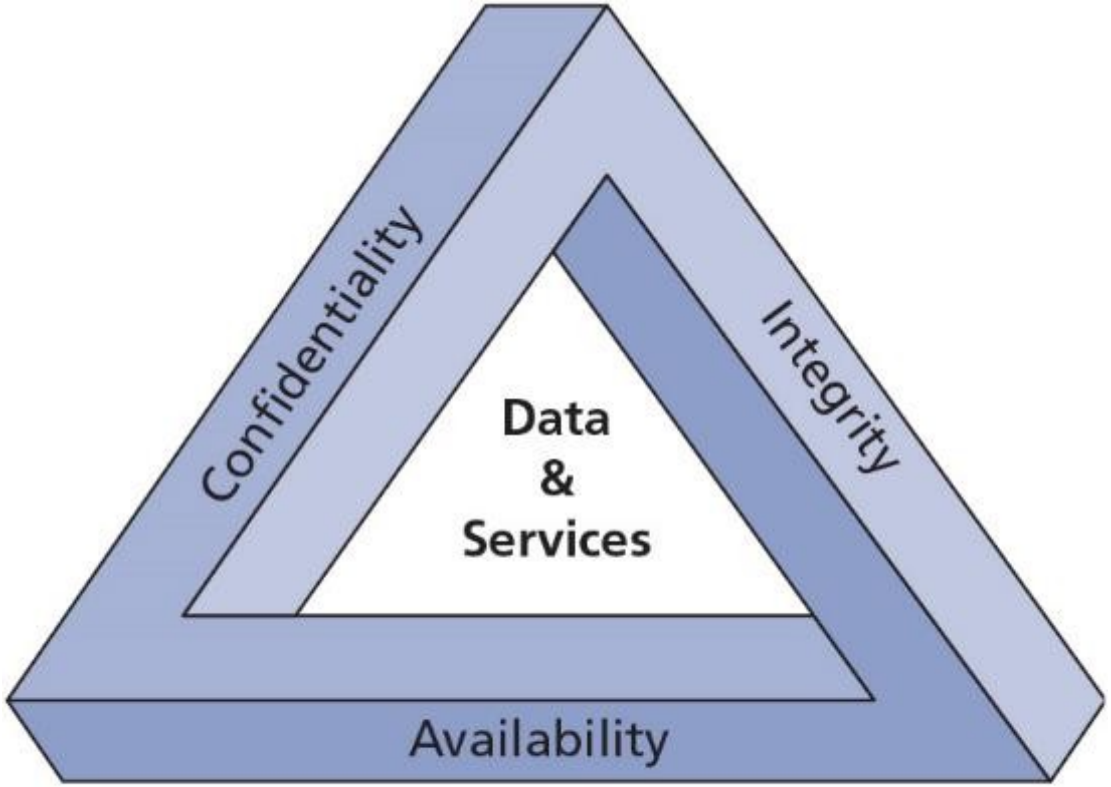


Figure 1-6 The C.I.A. triad

Key Information Security Concepts

- Access
- Asset
- Attack
- Control, safeguard, or countermeasure
- Exploit
- Exposure
- Loss
- Protection profile or security posture
- Risk
- Subjects and objects
- Threat
- Threat agent
- Threat event
- Threat source
- Vulnerability

Key Concepts in Information Security

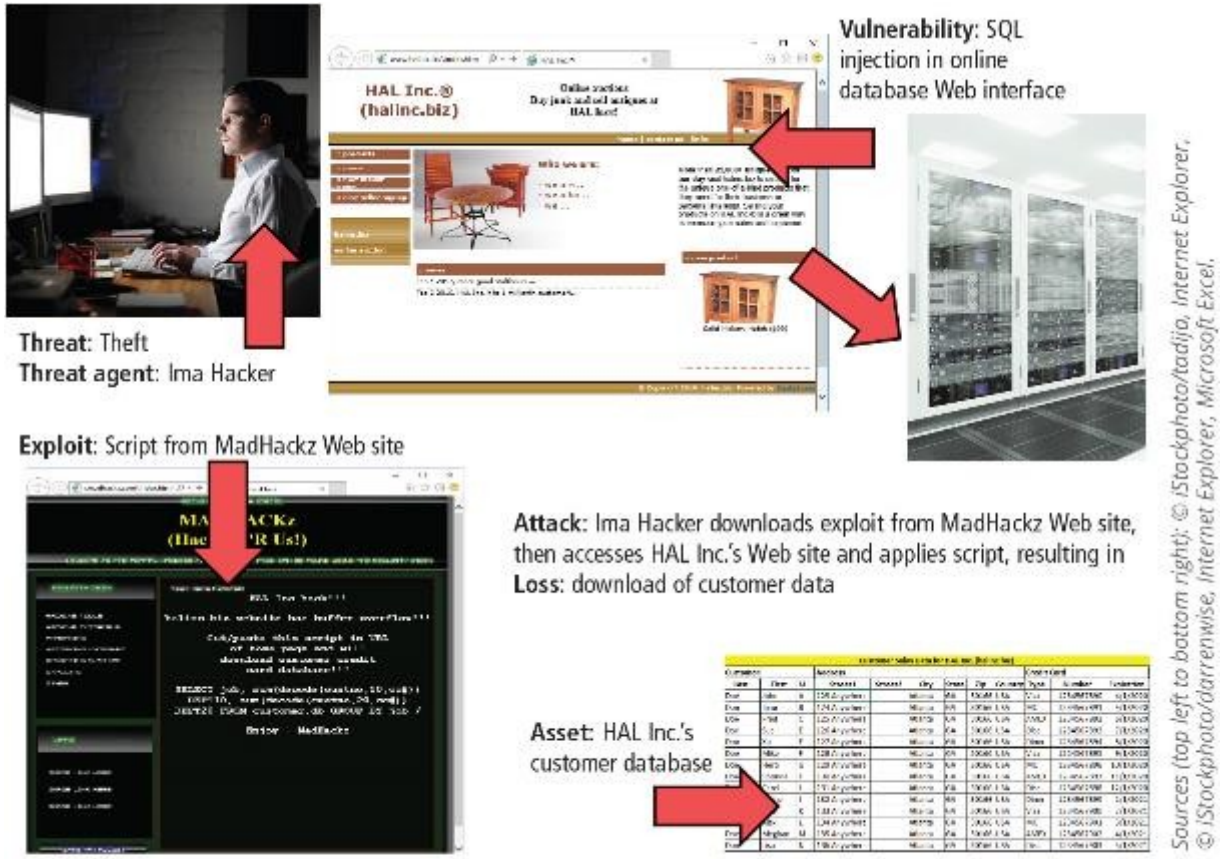


Figure 1-7 Key concepts in information security

Critical Characteristics of Information

- The value of information comes from the characteristics it possesses:
  - Confidentiality
  - Integrity
  - Availability
  - Accuracy
  - Authenticity
  - Utility
  - Possession

CNSS Security Model

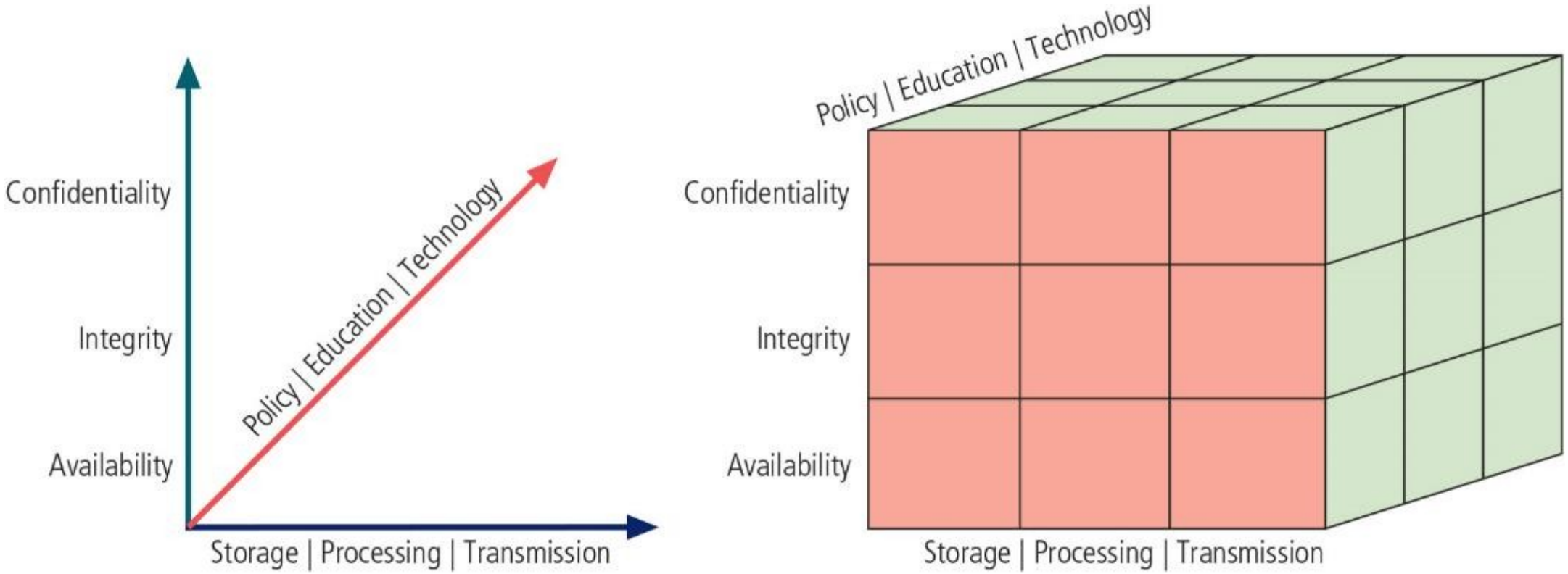


Figure 1-9 The McCumber Cube[14]

Components of an Information System

- An information system (IS) is the entire set of hardware, software data, people, procedures, and networks that enable a business to use information.
- All of them work together to support personal and professional operations.
- Each one has its own strengths and weaknesses, as well as its own characteristics and uses.
- Each one has its own security requirements.

Balancing Information Security and Access

- It is impossible to obtain perfect information security—it is a process, not a goal.
- Security should be considered a balance between protection and availability.
- To achieve balance, the level of security must allow reasonable access, yet protect against threats.

Approaches to Information Security Implementation: Bottom-Up Approach

- Grassroots effort: systems administrators work to improve security of their systems.
- Key advantage: technical expertise of individual administrators
- Seldom works, as it lacks a number of critical features:
  - Participant support
  - Organizational staying power

Approaches to Information Security Implementation: Top-Down Approach

- Initiated by upper management
  - Issue policy, procedures, and processes
  - Dictate goals and expected outcomes of project
  - Determine accountability for each required action
- The most successful type of top-down approach also involves a formal development strategy referred to as a systems development life cycle.

Approaches to Information Security Implementation

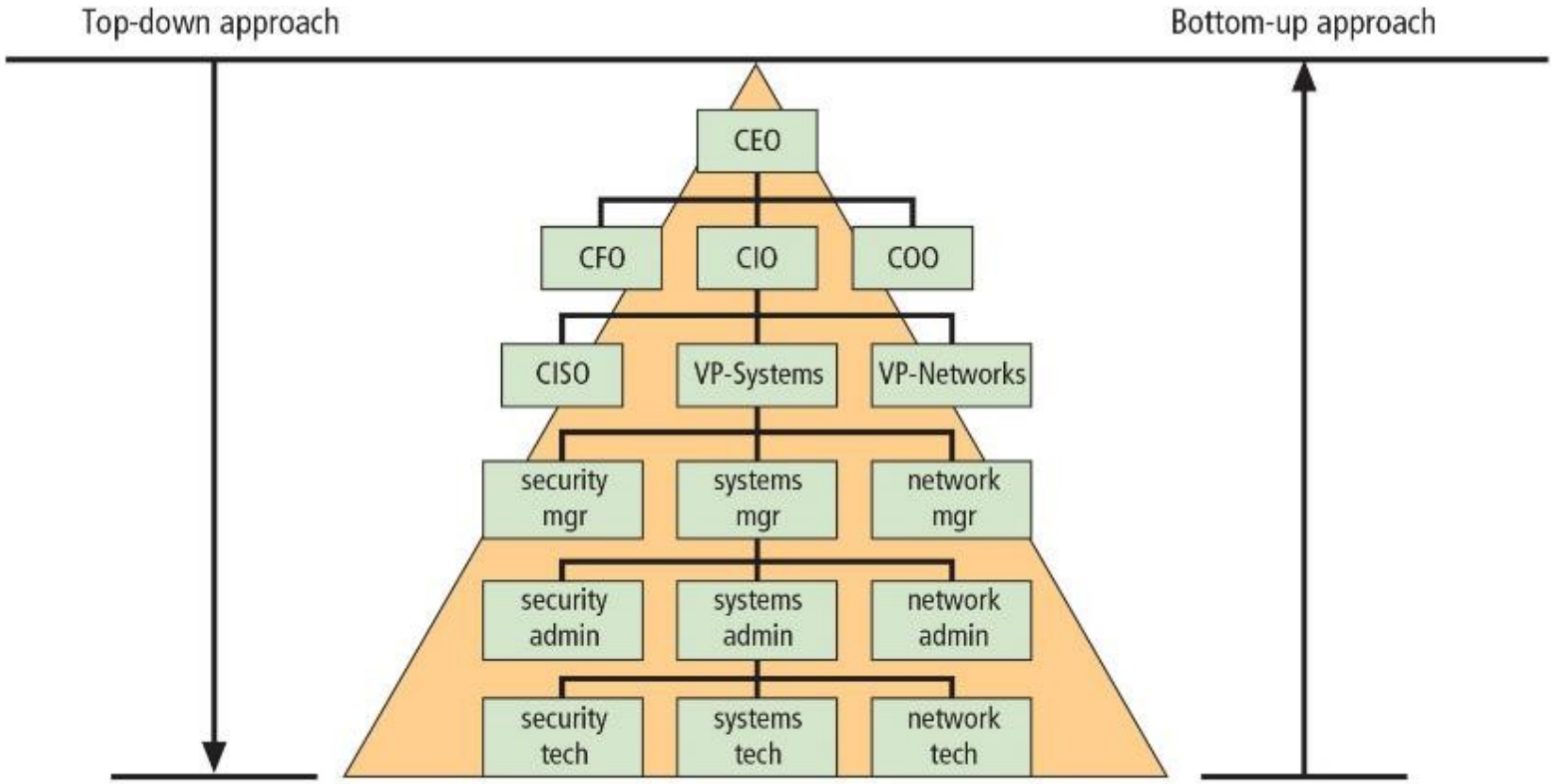


Figure 1-12 Approaches to information security implementation

Security Professionals and the Organization

- A wide range of professionals are required to support a diverse information security program.
- Senior management support is the key component.
- Additional administrative support and technical expertise are required to implement details of an IS program.

Senior Management

- Chief information officer (CIO)
  - Senior technology officer
  - Primarily responsible for advising the senior executives on strategic planning that affects the management of information in the organization
- Chief information security officer (CISO)
  - Has primary responsibility for assessment, management, and implementation of InfoSec in the organization
  - Usually reports directly to the CIO

Knowledge Check Activity 2

What title is given to the person with primary responsibility for assessment, management, and implementation of InfoSec in the organization?

a. CIO
b. CISO
c. CEO
d. CFO

Knowledge Check Activity 2: Answer

What title is given to the person with primary responsibility for assessment, management, and implementation of InfoSec in the organization?

Answer: B. CISO, or chief information security officer

The CISO usually reports to the CIO. While in some organizations, the CISO could report to the CFO, that is not common.

The CISO's Place and Roles

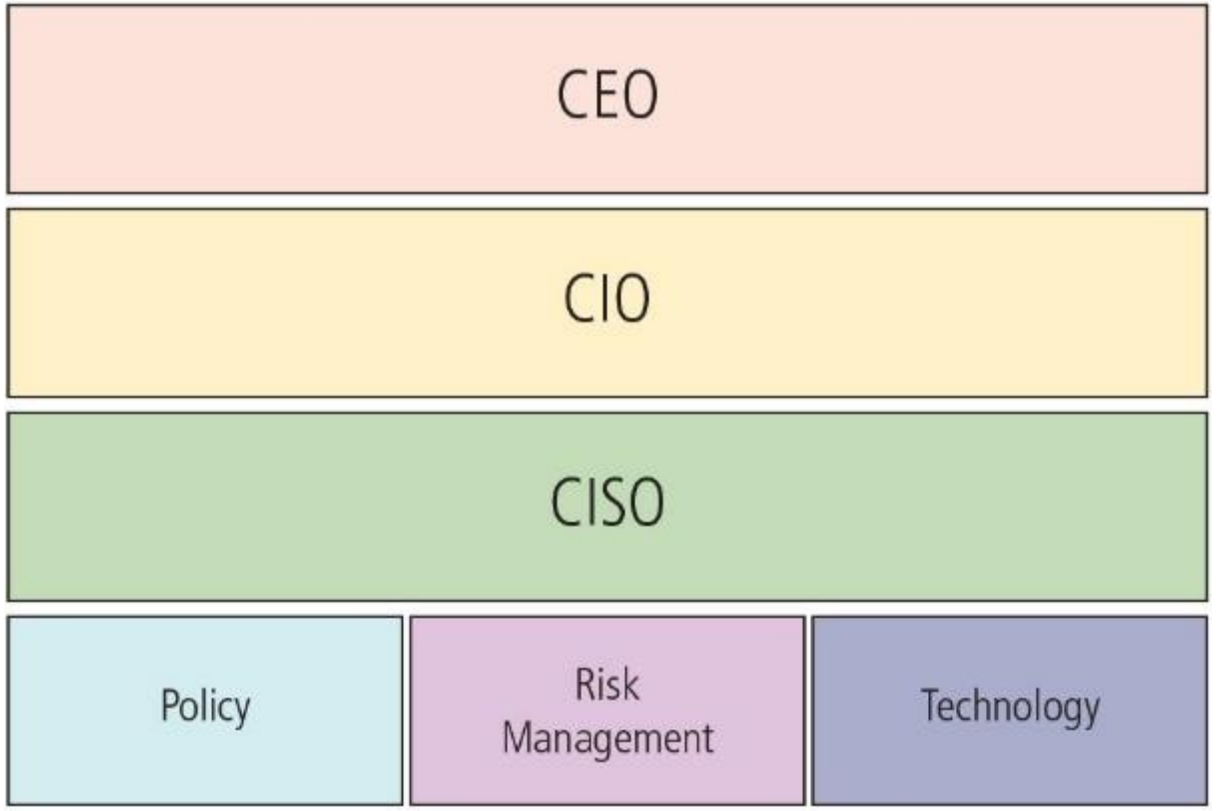


Figure 1-13 The CISO's place and roles

Information Security Project Team

- A small functional team of people who are experienced in one or multiple facets of required technical and nontechnical areas:
  - Champion
  - Team leader
  - Security policy developers
  - Risk assessment specialists
  - Security professionals
  - Systems administrators
  - End users

Data Responsibilities

- Data owners: senior management responsible for the security and use of a particular set of information
- Data custodian: responsible for information and systems that process, transmit, and store it
- Data trustees: appointed by data owners to oversee the management of a particular set of information and to coordinate with data custodians for its storage, protection, and use
- Data users: have access to information and thus an information security role

Knowledge Check Activity 3

Which group in the organization is appointed by data owners to oversee the management of a particular set of information and to coordinate with data custodians for its storage, protection, and use?

a. Data owners
b. Data custodian
c. Data trustee
d. Data user

Knowledge Check Activity 3: Answer

Which group in the organization is appointed by data owners to oversee the management of a particular set of information and to coordinate with data custodians for its storage, protection, and use?

Answer: C. Data trustee

Only this selection is correct since data owners would not appoint themselves, data custodians are responsible for the infrastructure that supports information processing in general, and data users do not have the responsibilities listed.

Communities of Interest

- Group of individuals united by similar interests/values within an organization
  - Information security management and professionals
  - Information technology management and professionals
  - Organizational management and professionals

Information Security: Is It an Art or a Science?

- Implementation of information security is often described as a combination of art and science.
- “Security artisan” idea: based on the way individuals perceive system technologists and their abilities
- Security as art: no hard and fast rules nor many universally accepted complete solutions; no manual for implementing security through entire system
- Security as science: technology is developed by scientists and engineers; specific conditions cause virtually all actions in computer systems; almost every security issue is a result of the interaction of specific hardware and software; with sufficient time, developers could resolve all faults.

Security as a Social Science

- Social science examines the behavior of individuals interacting with systems.
- Security begins and ends with the people that interact with the system, intentionally or otherwise.
- Security administrators can greatly reduce the levels of risk caused by end users and create more acceptable and supportable security profiles.

Summary (1 of 4)

- Information security evolved from the early field of computer security.
- Security is protection from danger. There are many types of security: physical security, personal security, operations security, communications security, national security, and network security, to name a few.
- Information security is the protection of information assets that use, store, or transmit information through the application of policy, education, and technology.
- The critical characteristics of information, including confidentiality, integrity, and availability (the C.I.A. triad), must be protected at all times. This protection is implemented by multiple measures that include policies, education, training and awareness, and technology.

Summary (2 of 4)

- Information systems are made up of the major components of hardware, software, data, people, procedures, and networks.
- Upper management drives the top-down approach to security implementation, in contrast with the bottom-up approach or grassroots effort, in which individuals choose security implementation strategies.

Summary (3 of 4)

- The control and use of data in the organization is accomplished by the following parties:
  - Data owners, who are responsible for the security and use of a particular set of information
  - Data custodians, who are responsible for the storage, maintenance, and protection of the information
  - Data trustees, who are appointed by data owners to oversee the management of a particular set of information and to coordinate with data custodians for its storage, protection, and use
  - Data users, who work with the information to perform their daily jobs and support the mission of the organization

Summary (4 of 4)

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

Self-Assessment

- What is information security?
- How has the concept of security for the use of computer systems changed over time?
- Information has many characteristics. What are the most critical of these characteristics that need to be kept secure?