COURSE TECHNOLOGY
CENGAGE Learning

Guide to Network Security
First Edition

Chapter One
Introduction to Information Security

About the Presentations

- The presentations cover the objectives found in the opening of each chapter.
- All chapter objectives are listed in the beginning of each presentation.
- You may customize the presentations to fit your class needs.
- Some figures from the chapters are included. A complete set of images from the book can be found on the Instructor Resources disc.

Objectives

- Explain the relationships among the component parts of information security, especially network security
- Define the key terms and critical concepts of information and network security
- Explain the business need for information and network security
- Identify the threats posed to information and network security, as well as the common attacks associated with those threats

Objectives (cont'd.)

- Distinguish between *threats* to information from within systems and *attacks* against information from within systems
- Describe the organizational roles of information and network security professionals
- Define management's role in the development, maintenance, and enforcement of information security policy, standards, practices, procedures, and guidelines

Objectives (cont'd.)

- Discuss how an organization institutionalizes policies, standards, and practices using education, training, and awareness programs

Introduction

- Network security
  - Critical to day-to-day IT operations of nearly every organization
- Information security
  - Field has matured in last 20 years
  - Large in scope

What is Information Security?

- Protection of information and its critical elements
  - Systems and hardware that use, store, and transmit information
- Information security includes:
  - Information security management
  - Computer and data security
  - Network security

What is Information Security? (cont'd.)

- Security layers
  - Network security
    - Protect components, connections, and contents
  - Physical items or areas
  - Personal security
    - Protect people
  - Operations security
    - Protect details of activities
  - Communications security
    - Protect media, technology, and content

Information Security Terminology

- Access
  - Ability to use, modify, or affect another object
- Asset
  - Organizational resource being protected
- Attack
  - Act that causes damage to information or systems
- Control, safeguard, or countermeasure
  - Security mechanisms, policies, or procedures

Information Security Terminology (cont'd.)

- Exploit
  - Technique used to compromise a system
- Exposure
  - Condition or state of being exposed to attack
- Intellectual property
  - Works of the mind
  - Inventions, literature, art, logos, and other creative works
- Loss
  - Single instance of damage to an information asset

Information Security Terminology (cont'd.)

- Protection profile or security posture
  - Set of controls that protect an asset
- Risk
  - Probability that something unwanted will happen
- Subject
  - Agent used to conduct the attack
- Object
  - Target entity of an attack

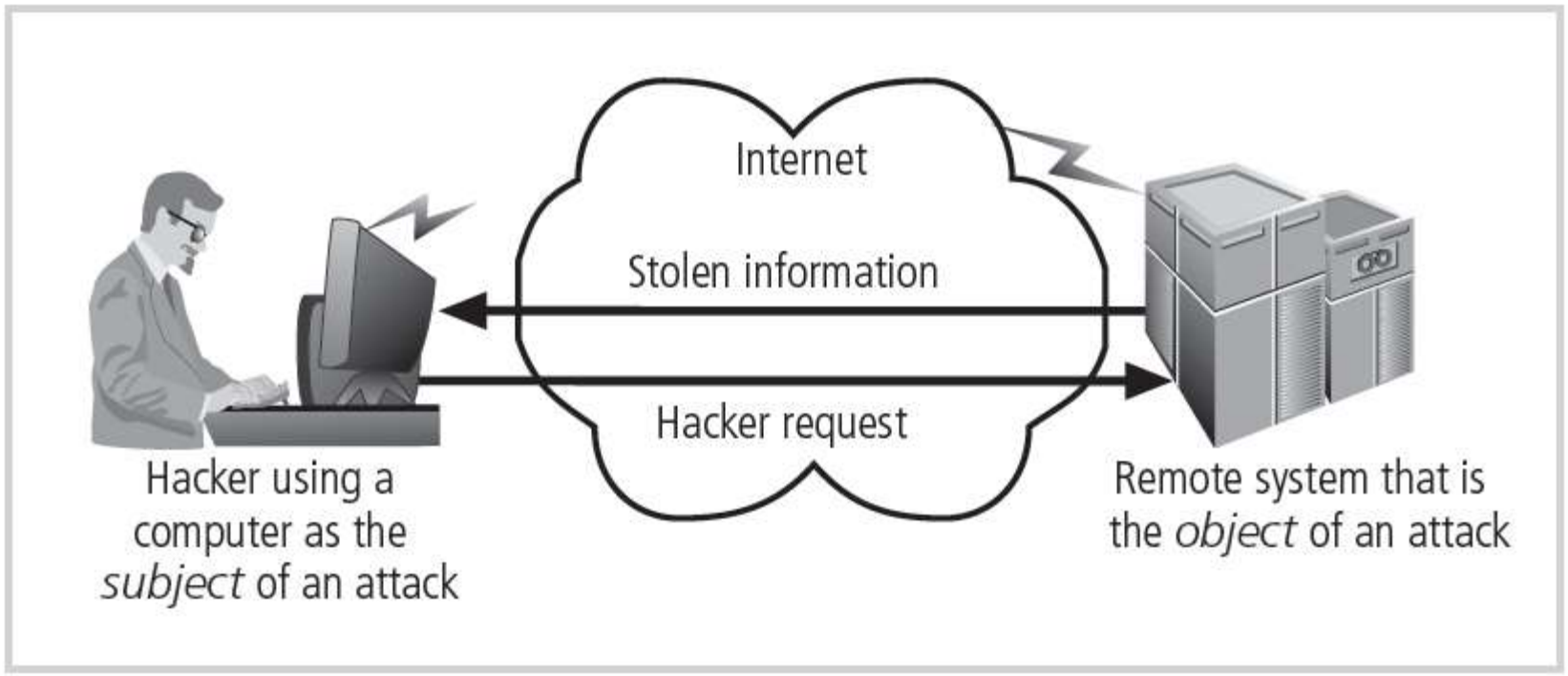

Figure 1-2 Computer as the subject and object of an attack
© Cengage Learning 2013

Information Security Terminology (cont'd.)

- Threat
  - Entity presenting danger to an asset
- Threat agent
  - Specific instance of a threat
  - Examples: lightning strike, tornado, or specific hacker
- Vulnerability
  - Weakness or fault in a system
  - Opens up the possibility of attack or damage

Critical Characteristics of Information

- Characteristics of information determine its value
- Availability
  - Ability to access information without obstruction
- Accuracy
  - Information is free from errors
- Authenticity
  - Quality or state of being genuine
- Confidentiality
  - Protection from disclosure to unauthorized individuals or systems

Critical Characteristics of Information (cont'd.)

- Data owners
  - Responsible for the security and use of a particular set of information
- Data custodians
  - Responsible for information storage, maintenance, and protections
- Data users
  - End users who work with information
- Integrity
  - Information remains whole, complete, uncorrupted

Critical Characteristics of Information (cont'd.)

- Utility
  - Information has value for some purpose or end
- Possession
  - Ownership or control of some object or item
- Privacy
  - Information is used in accordance with legal requirements

Security Models

- Information security model
  - Maps security goals to concrete ideas
- C.I.A. triad
  - Original basis of computer security

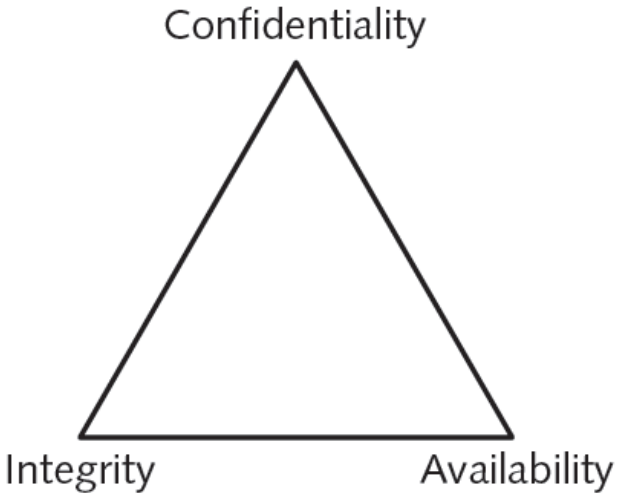

Figure 1-3 C.I.A. triad
© Cengage Learning 2013

Security Models (cont'd.)

- McCumber cube
  - Graphical description of architectural approach
  - Widely used in computer and information security
  - 27 cells represent areas to address to secure information systems

Security Models (cont'd.)

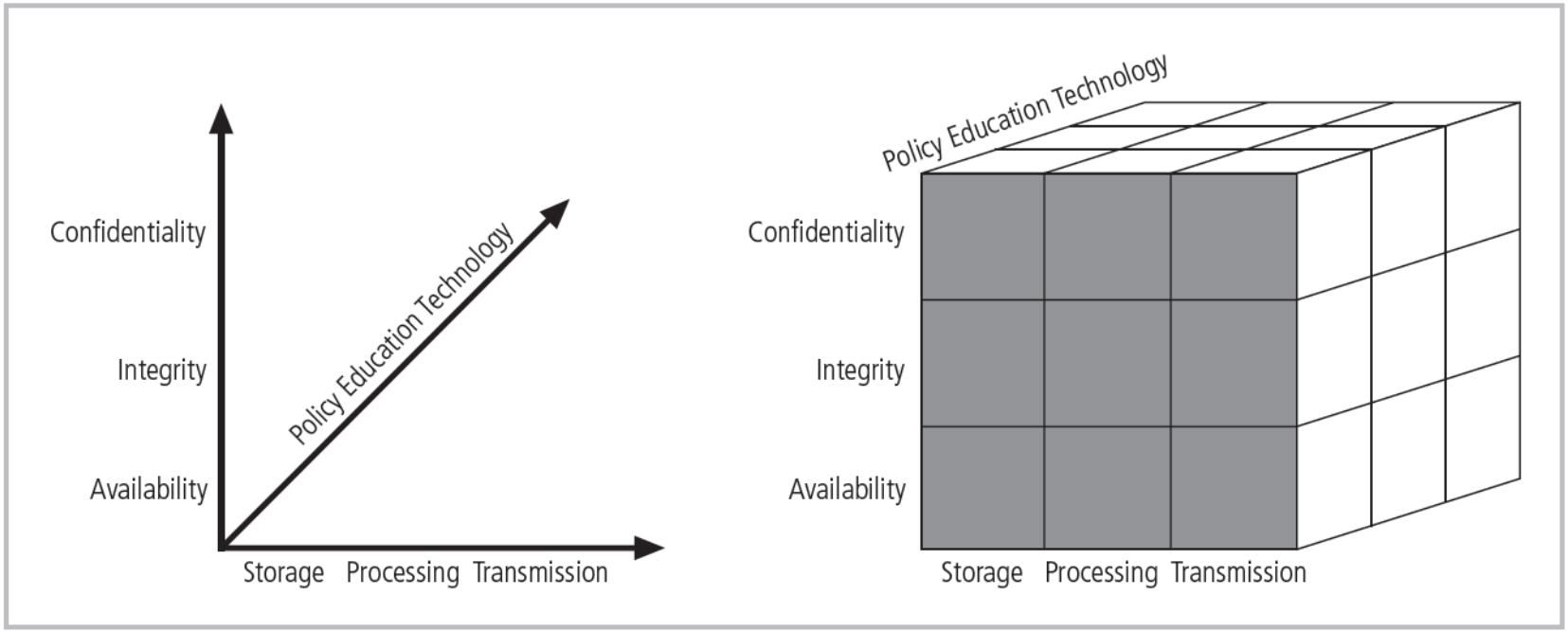

Figure 1-4 McCumber cube
© Cengage Learning 2013

Balancing Information Security and Access

- Information security must balance protection and availability
  - Allow reasonable access
  - Protect against threats
- Imbalance occurs when:
  - Needs of end user are undermined

Business Needs First

- Important organizational functions of an information security program
  - Protects organization's ability to function
  - Enables safe operation of applications
  - Protects data
  - Safeguards technology assets

Business Needs First (cont'd.)

- Protecting the functionality of an organization
  - General management and IT management are responsible
  - More to do with management than technology
- Enabling safe operation of applications
  - Securing storage of business-critical data
  - Ensuring integrity of key business transactions
  - Making communications constantly available

Business Needs First (cont'd.)

- Protecting data that organizations collect and use
  - Data in motion
  - Data at rest
- Safeguarding technology assets in organizations
  - Security should match size and scope of asset
  - Examples of assets: firewalls; caching network appliances

Threats to Information Security

- Wide range of threats pervade interconnected world
- Threats are relatively well researched
- See Table 1-1
  - 12 categories of danger to an organization's people, information, and systems

Category	Examples
1. Human error or failure	Accidents, employee mistakes, or failure to follow established policies or procedures
2. Compromises to intellectual property	Theft or unauthorized use of written documents, trade secrets, copyrights, trademarks, and patents, including software piracy
3. Espionage or trespass	Unauthorized access and/or data collection, hacking
4. Information extortion	Blackmail or information disclosure
5. Sabotage or vandalism	Destruction of systems or information
6. Theft	Illegal confiscation of equipment or information
7. Software attacks	Malicious code or malware attacks, including viruses, worms, macros, denial-of-service, Trojan horses
8. Forces of nature	Fire, flood, earthquake, lightning, and electrostatic discharge
9. Deviations in quality of service	ISP, power, or WAN service issues from service providers
10. Hardware failures or errors	Equipment failure
11. Software failures or errors	Bugs, code problems, unknown loopholes
12. Obsolescence	Antiquated or outdated technologies

Table 1-1 Threats to information security
© Cengage Learning 2013

Common Threats

- Cracker
  - Individual who “cracks” (removes) software protection
- Cyberterrorist
  - Hacks systems to conduct terrorist activities
- Hackers
  - Gain access without authorization
- Hacktivist or cyberactivist
  - Disrupts or interferes with operations to protest against an organization or government agency

Common Threats (cont'd.)

- Malicious code or malicious software
  - Computer viruses
    - Macro or boot virus
  - Worms
  - Trojan horses
  - Backdoor, trap door, or maintenance hook
  - Rootkit
- Packet monkeys
- Phreaker
  - Hacker who targets public telephone network

Common Threats (cont'd.)

- Script kiddies
  - Hackers of limited skill who use expertly written software to attack a system
- Shoulder surfing
  - Observing passwords of others
- Software piracy
  - Unlawful use or duplication of software IP

Attacks on Information Security

- Threats are always present
- Attacks occur through specific actions
  - May cause business loss

Malicious Code

- State-of-the-art malicious code attack
  - Polymorphic (or multivector) worm
  - Uses several attack vectors to exploit variety of vulnerabilities
  - See Table 1-2 for known attack vectors

Vector	Description
IP scan and attack	The infected system scans a random or local range of IP addresses and targets any of several vulnerabilities known to hackers or left over from previous exploits.
Web browsing	If the infected system has write access to any Web pages, it makes all Web content files (.html, .asp, .cgi, and others) infectious, so that users who browse to those pages become infected.
Virus	Each infected machine infects certain common executable or script files on all computers to which it can write with virus code that can cause infection.
Unprotected shares	Using vulnerabilities in file systems and the way many organizations configure them, the infected machine copies the viral component to all locations it can reach.
Mass mail	By sending e-mail infections to recipients in the address book, the infected machine infects many users, whose mail-reading programs also automatically run the program and infect other systems.
Simple Network Management Protocol (SNMP)	By using the common passwords that were employed in early versions of this protocol, widely used for remote management of network and computer devices, the attacker program can gain control of a device.

Table 1-2 Attack replication vectors
© Cengage Learning 2013

Password Attacks

- Password cracking
  - Attempt to bypass access controls
  - Guessing passwords
- Rainbow tables
  - Used when the hash of the user's password is known
- Brute force attacks
  - Trying every possible combination
- Dictionary
  - Trying specific, commonly used passwords

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks

- Denial-of-service attack
  - Attacker sends large number of requests to a target
  - Target system cannot handle volume of requests
  - System crashes
    - Or cannot handle legitimate requests
- Distributed denial-of-service attack
  - Coordinated stream of requests against a target
  - Occurs from many locations simultaneously

In a denial-of-service attack, a hacker compromises a system and uses that system to attack the target computer, flooding it with more requests for services than the target can handle.

In a distributed denial-of-service attack, dozens or even hundreds of computers (known as zombies) are compromised, loaded with DoS attack software, and then remotely activated by the hacker to conduct a coordinated attack.

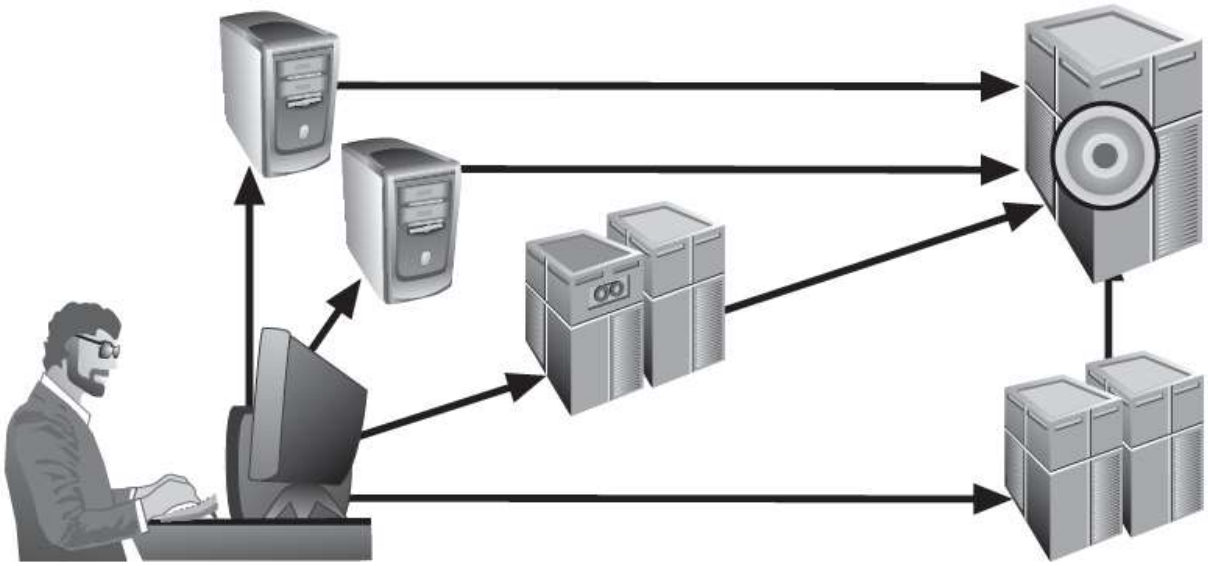

Figure 1-5 Denial-of-service attacks
© Cengage Learning 2013

Spoofing

- Technique used to gain unauthorized access to computers
- Intruder sends messages with fake IP address of a trusted host
  - Modifies the packet headers with the trusted IP
- Newer routers and firewalls can offer protection

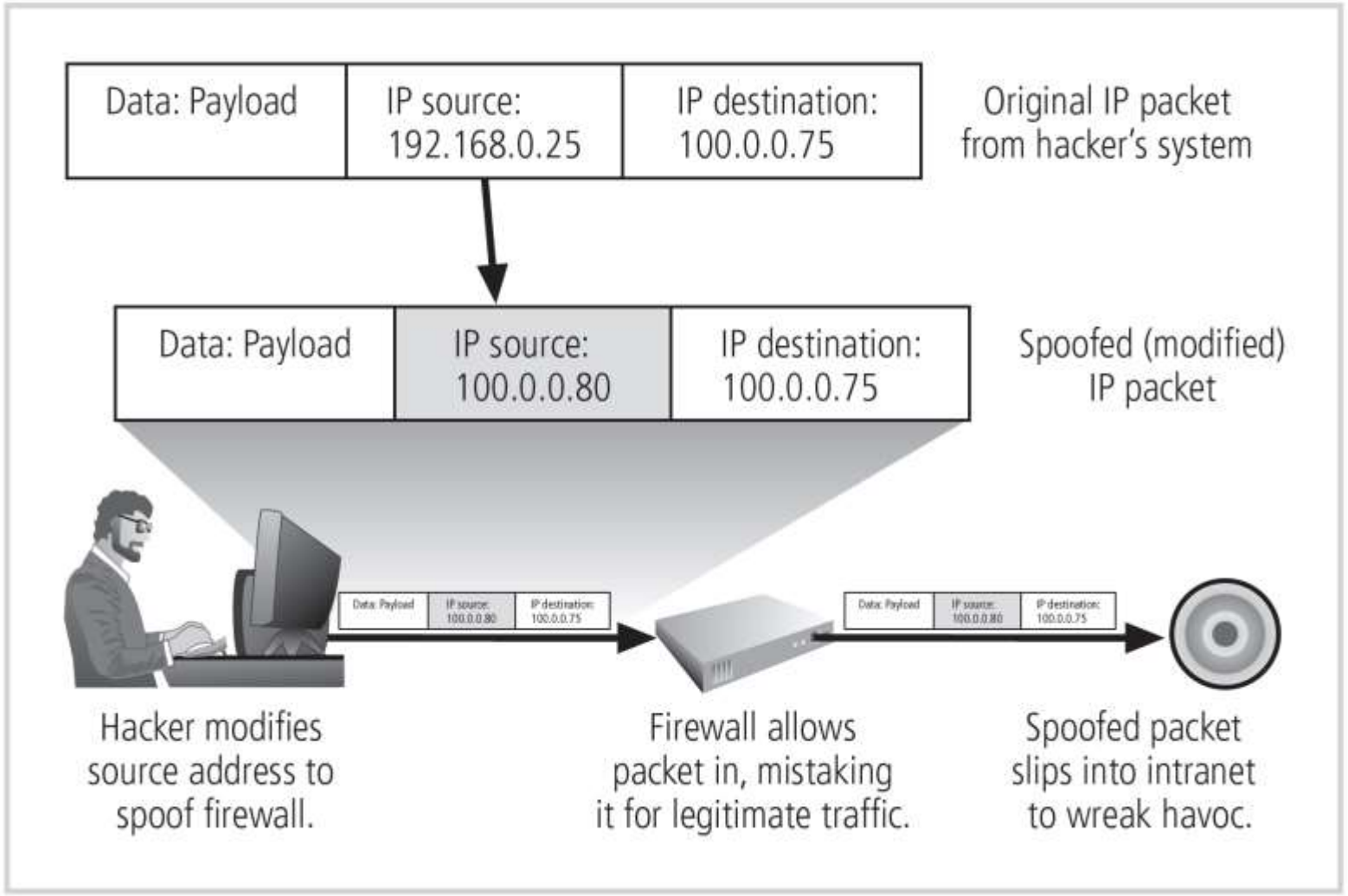

Figure 1-6 IP spoofing
© Cengage Learning 2013

Man-in-the-Middle Attacks

- Attacker monitors packets from the network
- Modifies packets using IP spoofing techniques
- Inserts packets back into network
- Can be used to eavesdrop, modify, reroute, forge, divert data

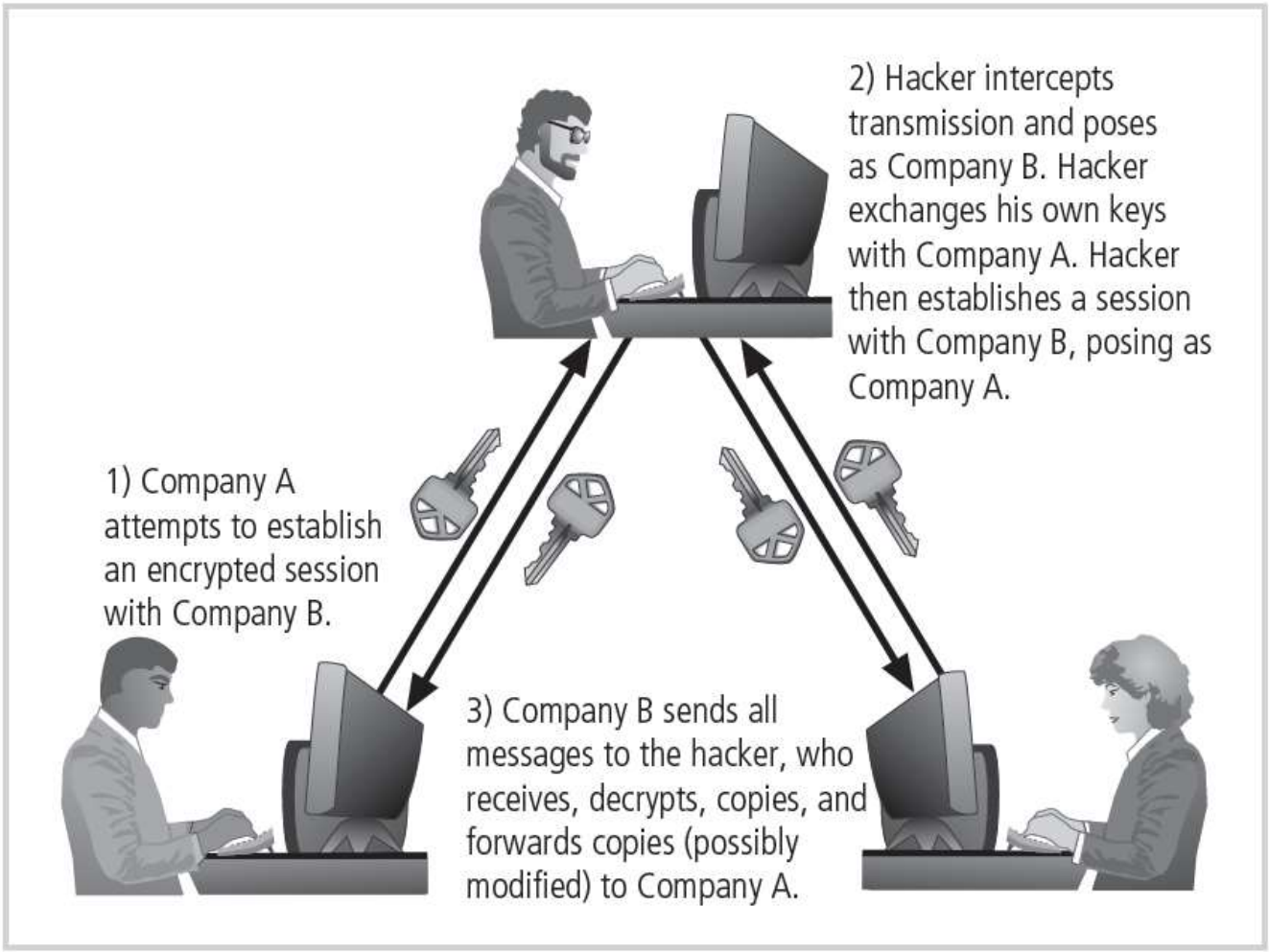

Figure 1-7 Man-in-the-middle attack
© Cengage Learning 2013

E-Mail Attacks

- Spam
  - Malicious code may be embedded in attachments
- Mail bomb
  - Attacker reroutes large quantities of e-mail to the target system
  - Poorly-configured e-mail systems at risk

Sniffers

- Program or device monitoring data traveling over a network
- Can be used for legitimate functions
  - Also for stealing information
- Unauthorized sniffers virtually impossible to detect
- Shows all data going by including passwords

Social Engineering

- Process of using social skills to convince people to reveal access credentials
- Usually involves impersonation
  - New employee
  - Employee who needs assistance
  - Someone higher in organizational hierarchy

Buffer Overflow

- Application error
- Occurs when more data is sent to a buffer than it can handle
- Attacker can take advantage of the consequence of the failure

Timing Attacks

- Measuring the time required to access a Web page
- Deducing that the user has visited the site before
  - Presence of the page in browser's cache
- Another type of timing attack:
  - Side channel attack on cryptographic algorithms

Security Professionals and the Organization

- Information security program
  - Supported by wide range of professionals
  - Administrative support also required
- Executive management
  - Chief information officer (CIO)
  - Chief information security officer (CISO)

Security Professionals and the Organization (cont'd.)

- Information security project team
  - Champion
  - Team leader
  - Security policy developers
  - Risk assessment specialists
  - Security professionals
  - Systems, network, and storage administrators
  - End users

Information Security Policy, Standards, and Practices

- Policy
  - Guidance implemented by senior management
  - Regulates activities
  - Similar to laws
- Standards
  - Detailed description of how to comply with policy
  - De facto standards
  - De jure standards

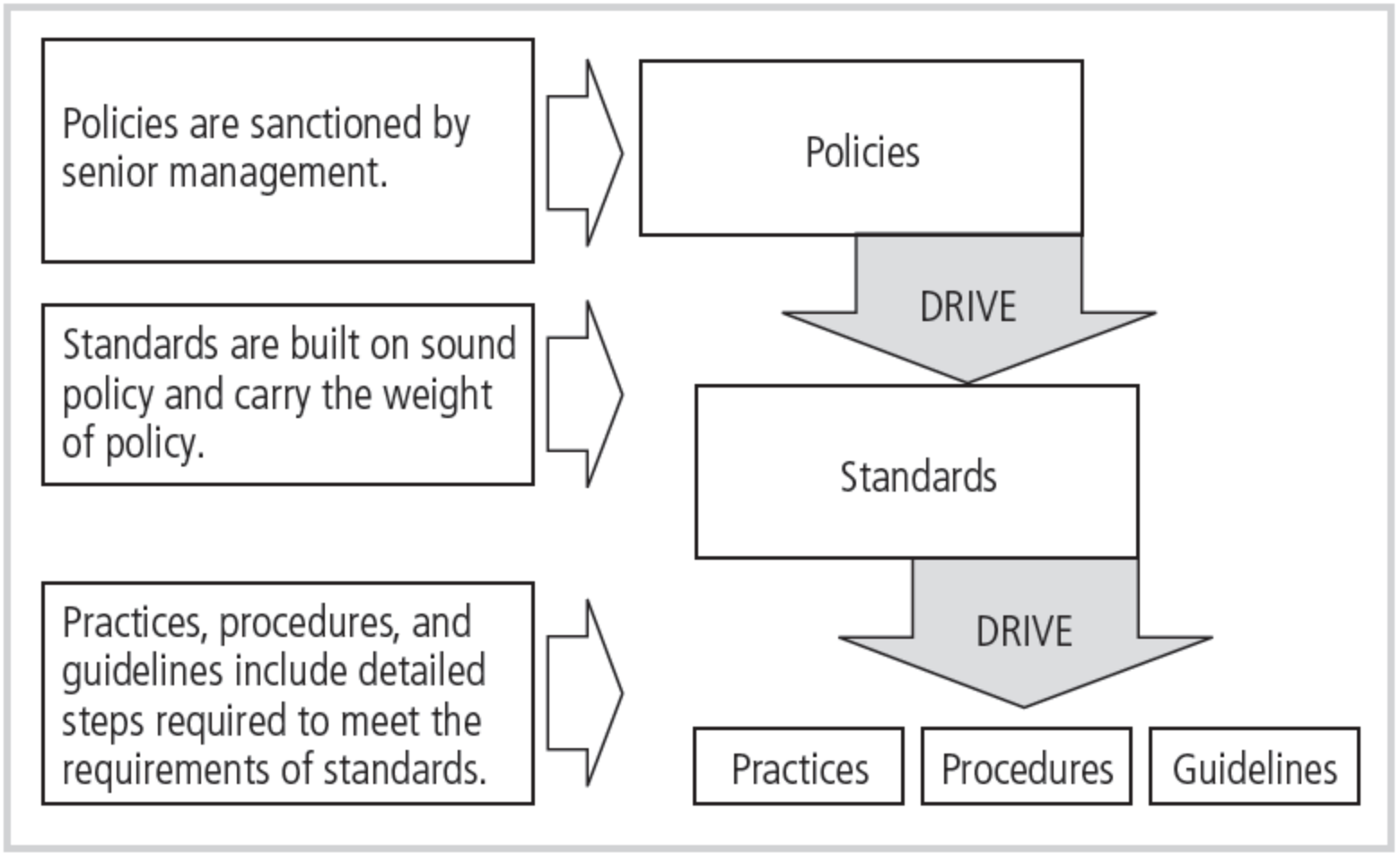

Figure 1-8 Policies, standards, and practices
© Cengage Learning 2013

Information Security Policy, Standards, and Practices (cont'd.)

- Management policy
  - Basis for information security planning, design, and deployment
- Criteria for effective policy
  - Dissemination
  - Review
  - Comprehension
  - Compliance
  - Uniformity

Enterprise Information Security Policy (EISP)

- Other names for EISP
  - General security policy
  - IT security policy
  - Information security policy
- Supports mission and vision of the organization
- Executive-level document
- Guides the security program
- Addresses legal compliance

Component	Description
Statement of Purpose	Answers the question "What is this policy for?" Provides a framework that helps the reader understand the document's intention. For example: "This document will: • Identify the elements of a good security policy • Explain the need for information security • Specify the various categories of information security • Identify the information security responsibilities and roles • Identify appropriate levels of security through standards and guidelines This document establishes an overarching security policy and direction for our company. Individual departments are expected to establish standards, guidelines, and operating procedures that adhere to and reference this policy while addressing their specific and individual needs."[22]
Information Technology Security Elements	Defines information security. For example: "Protecting the confidentiality, integrity, and availability of information while performing processing, transmission, and storage, through the use of policy, education and training, and technology." This section can also lay out security definitions or philosophies to clarify the policy.
Need for Information Technology Security	Provides information on the importance of information security in the organization and the obligation (legal and ethical) to protect critical information about customers, employees, and markets.
Information Technology Security Responsibilities and Roles	Defines the organizational structure designed to support information security. Identifies categories of individuals with responsibility for information security (IT department, management, users) and their information security responsibilities, including maintenance of this document.
Reference to Other Information Technology Standards and Guidelines	Lists other standards that influence and are influenced by this policy document, perhaps including relevant laws (federal and state) and other policies.

Table 1-3 Components of the EISP

© Cengage Learning 2013

Issue-Specific Security Policy (ISSP)

- States organization's position on each issue
- Examples of topics
  - Use of company-owned networks and the Internet
  - Use of e-mail
  - Prohibitions against hacking
  - Use of personal equipment on company networks

Table 1-4 Components of the ISSP

© Cengage Learning 2013

Component	Description
1. Statement of policy a. Scope and applicability b. Definition of technology addressed c. Responsibilities	The policy should begin with a clear statement of purpose.
2. Authorized access and usage a. User access b. Fair and responsible use c. Protection of privacy	Who can use the technology governed by the policy, and what can it be used for? An organization's information systems are the exclusive property of the organization, and users have no general rights of use. Each technology and process is provided for business operations. Use for any other purpose constitutes misuse.
3. Prohibited usage a. Disruptive use or misuse b. Criminal use c. Offensive or harassing materials d. Copyrighted, licensed, or other intellectual property e. Other restrictions	Unless a particular use is clearly prohibited, the organization cannot penalize its employees for using it in that fashion.
4. Systems management a. Management of stored materials b. Employer monitoring c. Virus protection d. Physical security e. Encryption	All systems-management responsibilities should be designated to the systems administrators or to the users; otherwise, each may infer that the responsibility belongs to the other.
5. Violations of policy a. Procedures for reporting violations b. Penalties for violations	Users need to be instructed how to report suspected violations of policy. Allowing anonymous submissions may be the only way to convince them to report the unauthorized activities of other, more influential employees.
6. Policy review and modification a. Scheduled review of policy and procedures for modification	Each policy should contain procedures and a timetable for periodic reviews so that users do not begin circumventing policy as it grows obsolete.
7. Limitations of liability a. Statements of liability or disclaimers	The policy should state that the organization will not protect employees who violate a company policy or any law using company technologies, and that the company is not liable for such actions.

Systems-Specific Policy (SysSP)

- Managerial guidance SysSPs
  - Guides technology implementation and configuration
  - Regulates behavior of people in organization
- Technical specification SysSPs
  - Access control lists
  - Capability table
  - Access control matrix
- Configuration rule policies
  - Specific instructions to regulate security system

Frameworks and Industry Standards in Information Security

- Security blueprint
  - Used to implement the security program
  - Basis for design, selection, and implementation of program elements
- Security framework
  - Outline of overall information security strategy
  - Roadmap for planned changes to the environment
- Security models
  - Can be used to develop a security blueprint

The ISO 27000 series

- One of the most widely referenced security models
- Gives recommendations for information security management
- See Figure 1-9 for overall methodology

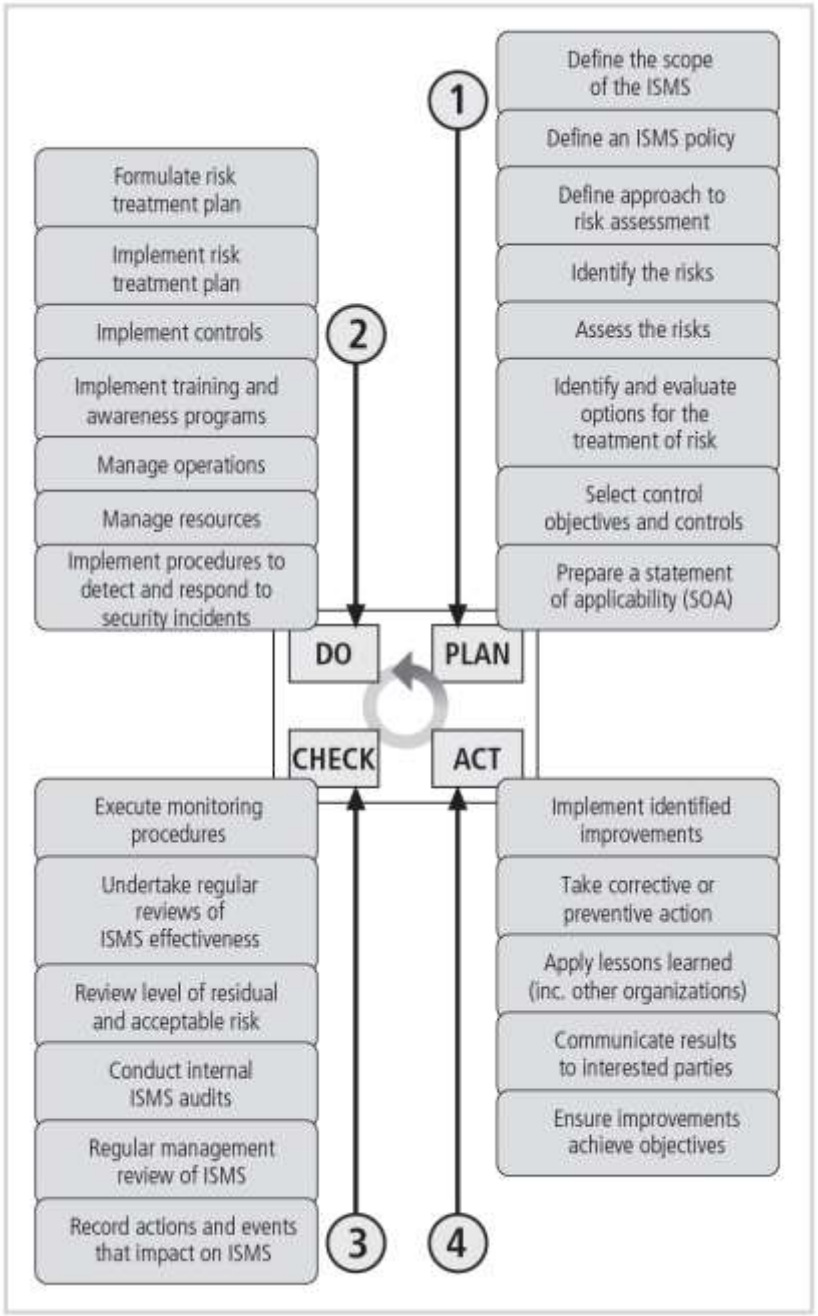

Figure 1-9 ISO/IEC 27002 major process steps
© Cengage Learning 2013

Standard	Status	Title or Topic	Comment
27000	Published 2009	Series Overview and Vocabulary	Typically, when ISO releases a series of standards, the first defines series terminology and vocabulary
27001	Published 2005	Information Security Management System Specification	Drawn from BS 7799:2
27002	Published 2010	Code of Practice for Information Security Management	Was renamed from ISO/IEC 17799, drawn from BS 7799:1
27003	Published 2010	Information Security Management Systems Implementation Guidelines	To provide guidance and assistance in implementing an ISMS
27004	Published 2009	Information Security Measurements and Metrics	To assist organizations in collecting, evaluating, and reporting metrics and performance measures
27005	Published 2008	ISMS Risk Management	Guidelines for InfoSec Risk Management—supporting requirement of ISO 27001
27006	Published 2007	Requirements for Bodies Providing Audit and Certification of an ISMS	Largely intended to support the accreditation of certification bodies providing ISMS certification
27007	Planned	InfoSec Management Systems Auditing	In preparation
27008	Planned	InfoSec Management Auditing – Security Controls	In preparation
27011	Published 2008	IT: InfoSec Management Guidelines for Telecomm	ISMS assistance for the implementation of InfoSec management in Telecom organizations

Table 1-6 ISO 27000 series current and planned standards (www.27000.org)
© Cengage Learning 2013

NIST Security Models

- Available from csrc.nist.gov
- Publicly available
- Free
- Reviewed by government and industry professionals
- Many documents available

IETF Security Architecture

- Security area working group
  - Acts as advisory board for IETF
- RFC 2196: Site security handbook
  - Good reference
  - Covers five basic areas of security

Benchmarking and Best Business Practices

- Methods used by some organizations
  - To assess security practices
- Federal Agency Security Practices Web site
  - Popular resource for best practices
- SANS Institute
  - Cooperative information security research organization
- Other sources
  - www.cert.org
  - http://www.us-cert.gov

Benchmarking and Best Business Practices (cont'd.)

- Spheres of security
  - Shows that information is at risk from various sources
  - Illustrated in Figure 1-10
- Defense in depth
  - Layered implementation of security
  - Organization establishes multiple layers of security controls

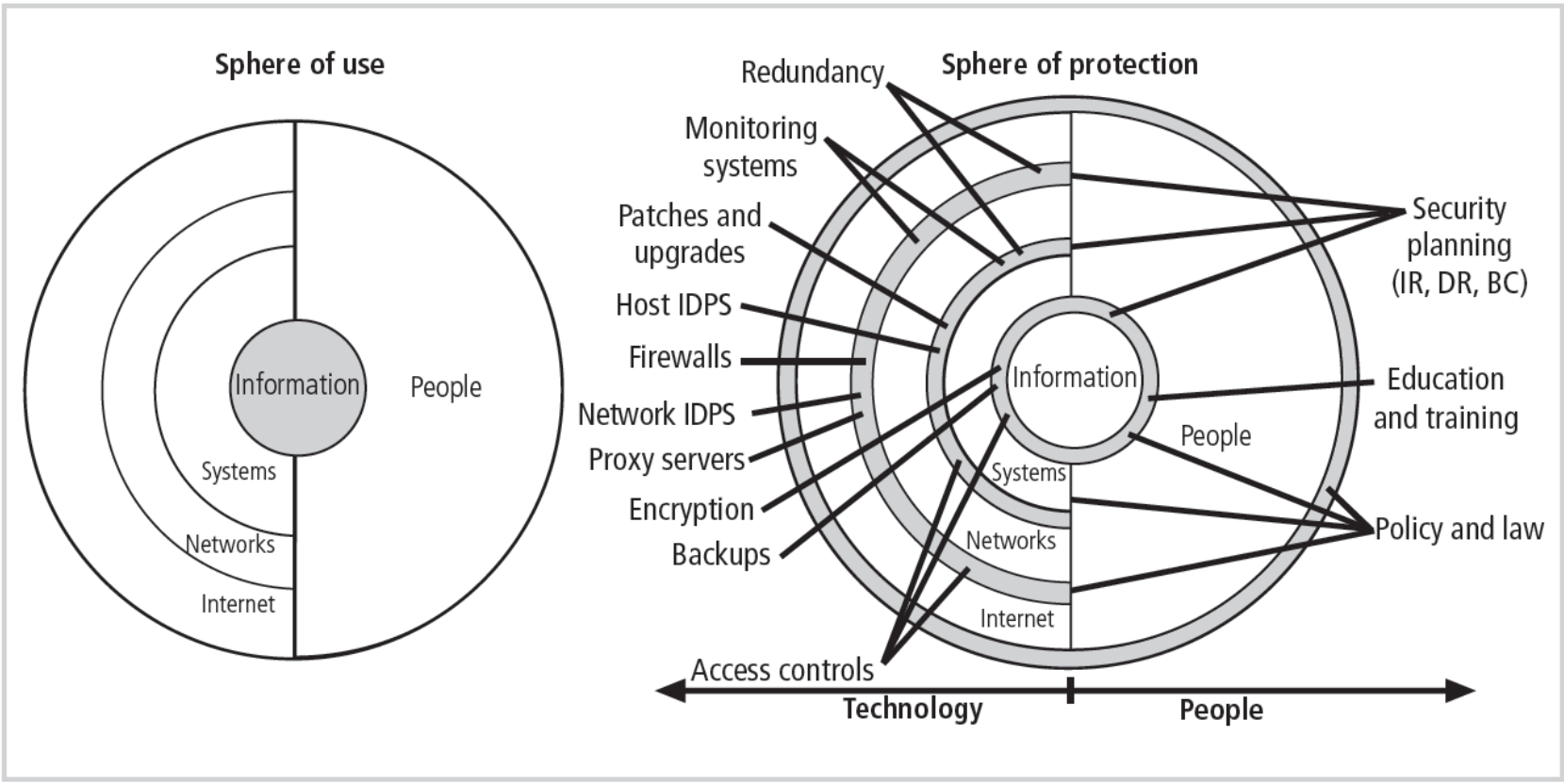

Figure 1-10 Spheres of security

© Cengage Learning 2013

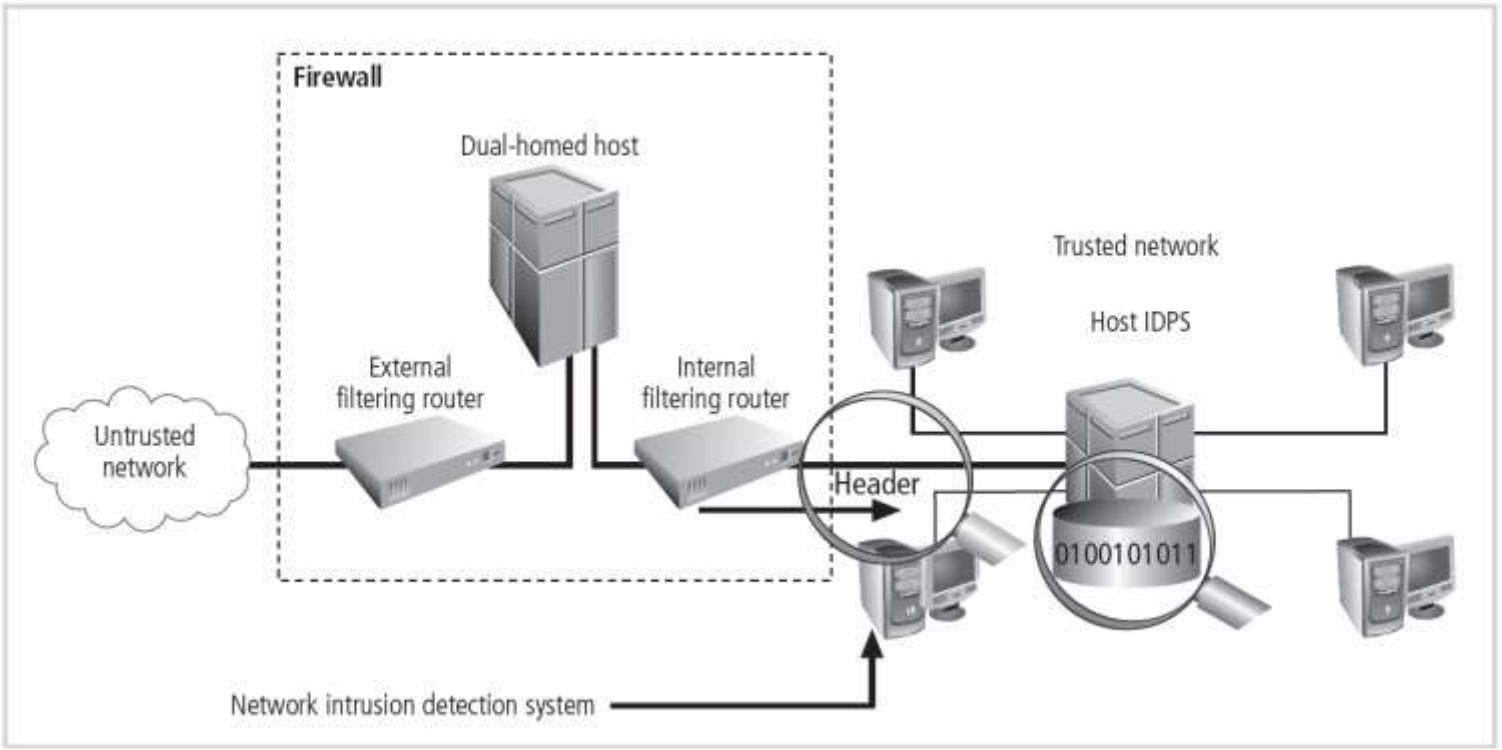

Figure 1-11 Defense in depth

© Cengage Learning 2013

Benchmarking and Best Business Practices (cont'd.)

- Redundancy
  - Implementing multiple types of technology
    - Prevents failure of one system from compromising security of another system
- Security perimeter
  - Defines the boundary between organization's security and outside world
  - Both electronic and physical

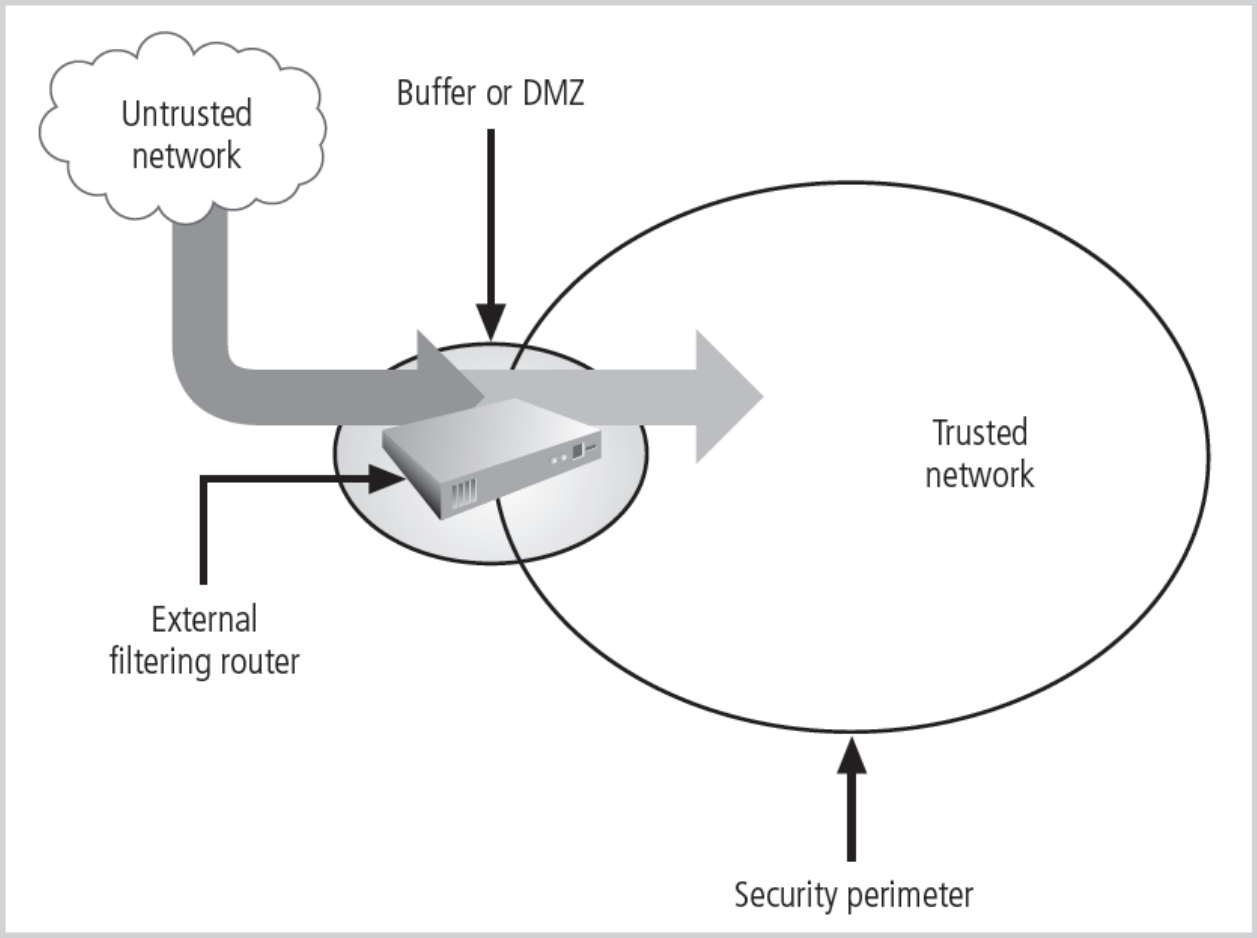

Figure 1-12 Security perimeters
© Cengage Learning 2013

Summary

- Information security is the protection of information
  - Information value comes from its characteristics
- A threat is an object, person, or entity that represents a danger to an asset
- An attack is an action that takes advantage of a vulnerability to compromise a controlled system
- Security models include the C.I.A. triad and the McCumber cube

Summary (cont'd.)

- Information security functions
  - Protects organization's ability to function
  - Enables safe operation of applications
  - Protects data
  - Safeguards technology assets
- Many types of professionals support an information security program
- Management policy is the basis for all information security planning