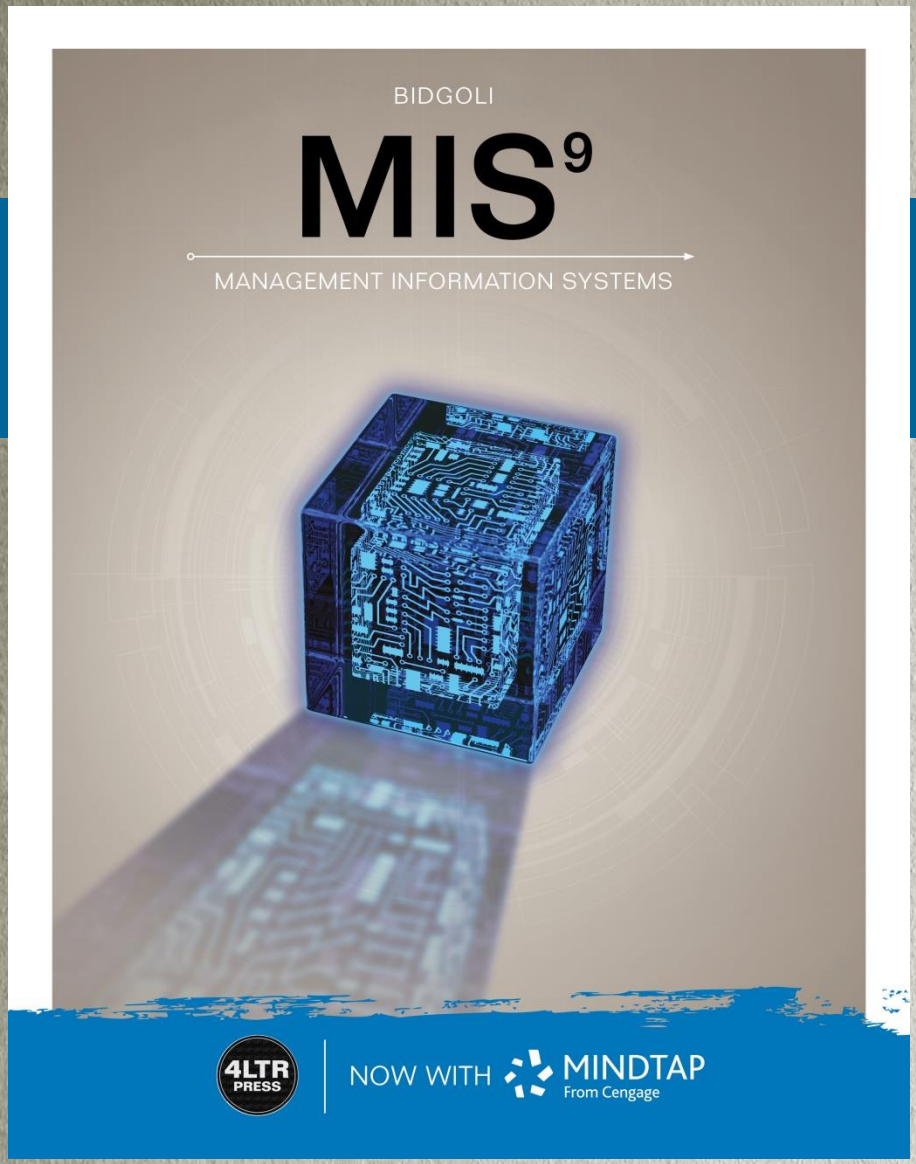


5

Protecting Information Resources

Learning Objectives (1 of 2)

- Describe information technologies that could be used in computer crimes
- Describe basic safeguards in computer and network security
- Explain the major security threats
- Describe security and enforcement measures

Learning Objectives (2 of 2)

- Summarize the guidelines for a comprehensive security system, including business continuity planning

Risks Associated with Information Technologies

- Information technologies can be misused to invade users' privacy and commit computer crimes
  - You can minimize or prevent many of these risks by installing operating system updates regularly, using antivirus and antispyware software, and using e-mail security features

The Costs of Cyber Crime to the U.S. Economy

- Costs include:
  - Stolen identities, intellectual property, and trade secrets
  - Damage done to companies' and individuals' reputations
  - Expense of enhancing and upgrading a company's network security after an attack
  - Opportunity costs associated with downtime and lost trust and loss of sensitive business information

Spyware and Adware

- Spyware
  - Software that secretly gathers information about users while they browse the Web
    - Prevented by installing antivirus or antispyware software
- Adware
  - Spyware that collects information about the user to determine advertisements to display
    - Prevented by installing an ad-blocking feature in the Web browser

Phishing, Pharming, Baiting, Quid Pro Quo, SMiShing, and Vishing (1 of 3)

- Phishing
  - Sending fraudulent e-mails that seem to come from legitimate sources
- Pharming
  - Internet users are directed to fraudulent Web sites with the intention of stealing their personal information

Phishing, Pharming, Baiting, Quid Pro Quo, SMiShing, and Vishing (2 of 3)

- Baiting
  - Similar to phishing attacks; baiter gives recipient a promise
- Quid pro quo
  - Involves a hacker requesting the exchange of critical data or login information in exchange for a service or prize

Phishing, Pharming, Baiting, Quid Pro Quo, SMiShing, and Vishing (3 of 3)

- SMiShing (SMS phishing)
  - Technique tricks a user to download a malware
- Vishing (voice or VoIP phishing)
  - Technique tricks a user to reveal important financial or personal information to unauthorized entities

Keystroke Loggers

- Monitor and record keystrokes
  - Can be software or hardware devices
  - Used by companies to track employees' use of e-mail and the Internet
  - Used for malicious purposes
  - Prevented by some antivirus and antispyware programs

Sniffing and Spoofing

- Sniffing
  - Capturing and recording network traffic
  - Used by hackers to intercept information
- Spoofing
  - Attempting to gain access to a network by posing as an authorized user in order to find sensitive information
  - Also happens when an illegitimate program poses as a legitimate one

Computer Crime and Fraud (1 of 2)

- Computer fraud
  - Unauthorized use of computer data for personal gain
- Computer crimes
  - Denial-of-service attacks
  - Identity theft and software piracy
  - Distributing child pornography
  - E-mail spamming
  - Writing or spreading malicious codes

Computer Crime and Fraud (2 of 2)

- Stealing files for industrial espionage
- Changing computer records illegally
- Virus hoaxes
- Sabotage
- Holding a firm's critical data for ransom
  - Example: ransomware

Computer and Network Security: Basic Safeguards (1 of 5)

- Comprehensive security system
  - Protects an organization's resources
  - Collectively protect information resources and keep intruders and hackers at bay
    - Hardware
    - Software
    - Procedures
    - Personnel

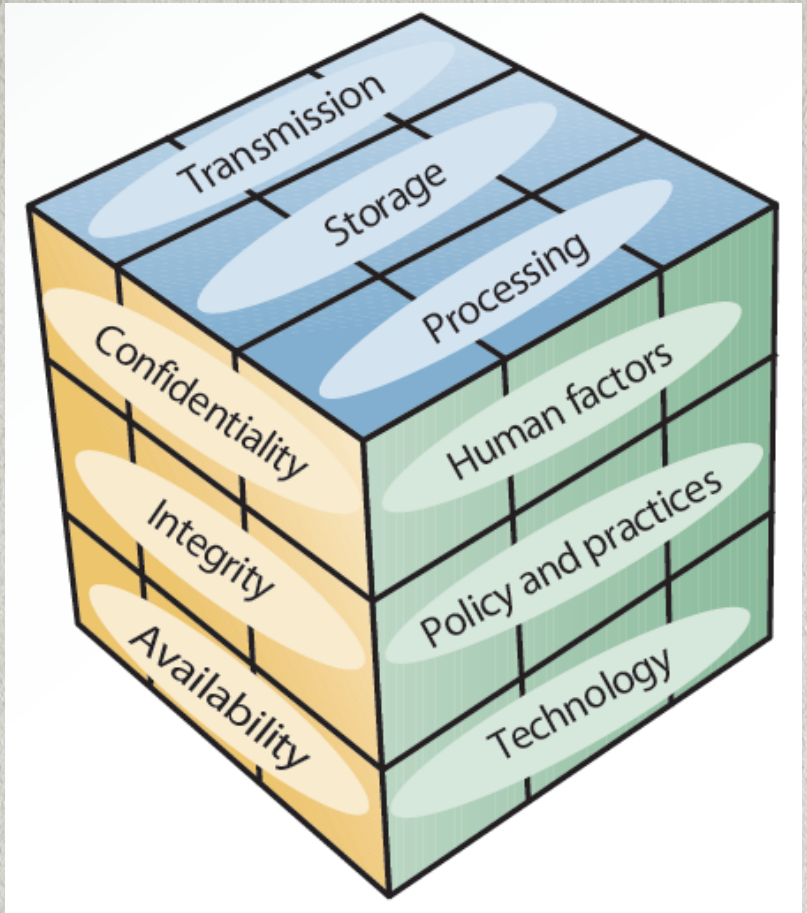
Computer and Network Security: Basic Safeguards (2 of 5)

- Important aspects of computer and network security: CIA triangle
  - Confidentiality
  - Integrity
  - Availability

Computer and Network Security: Basic Safeguards (3 of 5)

- McCumber cube
  - Framework for evaluating information security
  - Represented as a three-dimensional cube
  - Defines nine characteristics of information security
  - Includes different states in which information can exist in a system
    - Transmission, storage, and processing

Exhibit 5.1 McCumber Cube



Computer and Network Security: Basic Safeguards (4 of 5)

- Levels of network security
  - Level 1: front-end servers
    - Protected against unauthorized access
  - Level 2: back-end systems
    - Protected to ensure data confidentiality, accuracy, and integrity
  - Level 3: corporate network
    - Protected against intrusion, denial-of-service attacks, and unauthorized access

Computer and Network Security: Basic Safeguards (5 of 5)

- Planning a comprehensive security system: designing fault-tolerant systems
  - Ensure availability in the event of a system failure by using a combination of hardware and software
  - Commonly used methods
    - Uninterruptible power supply (UPS)
    - Redundant array of independent disks (RAID)
    - Mirror disks

Intentional Threats

- Intentional threats include:
  - Viruses and worms
  - Trojan programs
  - Logic bombs
  - Backdoors
  - Blended threats
  - Rootkits
  - Denial-of-service attacks
  - Social engineering

Viruses

- Consists of self-propagating program code that is triggered by a specified time or event
  - Attaches itself to other files, and the cycle continues when the program or operating system containing the virus is used
  - Transmitted through a network or e-mail attachments, or message boards
  - Prevented by installing and updating an antivirus program

Worms

- Independent programs that can spread themselves without having to be attached to a host program
  - Replicate into a full-blown version that could end up eating computing resources
  - Examples: Code Red, Melissa, and Sasser

Trojan Programs

- Contain code intended to disrupt a computer, network, or Web site
  - Hidden inside a popular program

Logic Bombs

- Type of Trojan program used to release a virus, worm, or other destructive code
  - Triggered at a certain time or by a specific event

Backdoors

- Programming routine built into a system by its designer or programmer
  - Enables the designer or programmer to bypass security and sneak back into the system later to access programs or files

Blended Threats

- Combines characteristics of viruses, worms, and malicious codes with vulnerabilities on networks
  - Search for vulnerabilities in computer networks and take advantage of them
    - Embedding malicious codes in the server's HTML files
    - Sending unauthorized e-mails from compromised servers with a worm attachment

Denial-of-Service Attacks (1 of 2)

- Flood a network or server with service requests to prevent legitimate users' access to the system
  - Distributed denial-of-service (DDoS) attack: thousands of computers work together to bombard a Web site with thousands of requests in a short period, causing it to grind to a halt

Denial-of-Service Attacks (2 of 2)

- Botnet: network of computers and IoT devices:
  - Infected with malicious software
  - Controlled as a group without owners' knowledge
- TDoS (telephony denial of service) attacks
  - Use high volumes of automated calls to tie up a target phone system, halting incoming and outgoing calls

Social Engineering

- Using "people skills" to trick others into revealing private information
- Commonly used social-engineering techniques
  - Dumpster diving
  - Shoulder surfing
  - Tailgating
  - Scareware
  - Pretexting

Security Measures And Enforcement: An Overview

- Components of a comprehensive security system
  - Biometric, nonbiometric, and physical security measures
  - Access controls
  - Virtual private networks
  - Data encryption
  - E-commerce transaction security measures
  - Computer Emergency Response Team (CERT)

Biometric Security Measures

- Use a physiological element unique to a person that cannot be stolen, lost, copied, or passed on to others
  - Biometric devices and measures
    - Facial recognition, fingerprints, hand geometry, iris analysis, palm prints, retinal scanning, signature analysis, vein analysis, and voice recognition

Nonbiometric Security Measures

- Three main nonbiometric security measures
  - Callback modems
  - Firewalls
  - Intrusion detection systems

Callback Modems

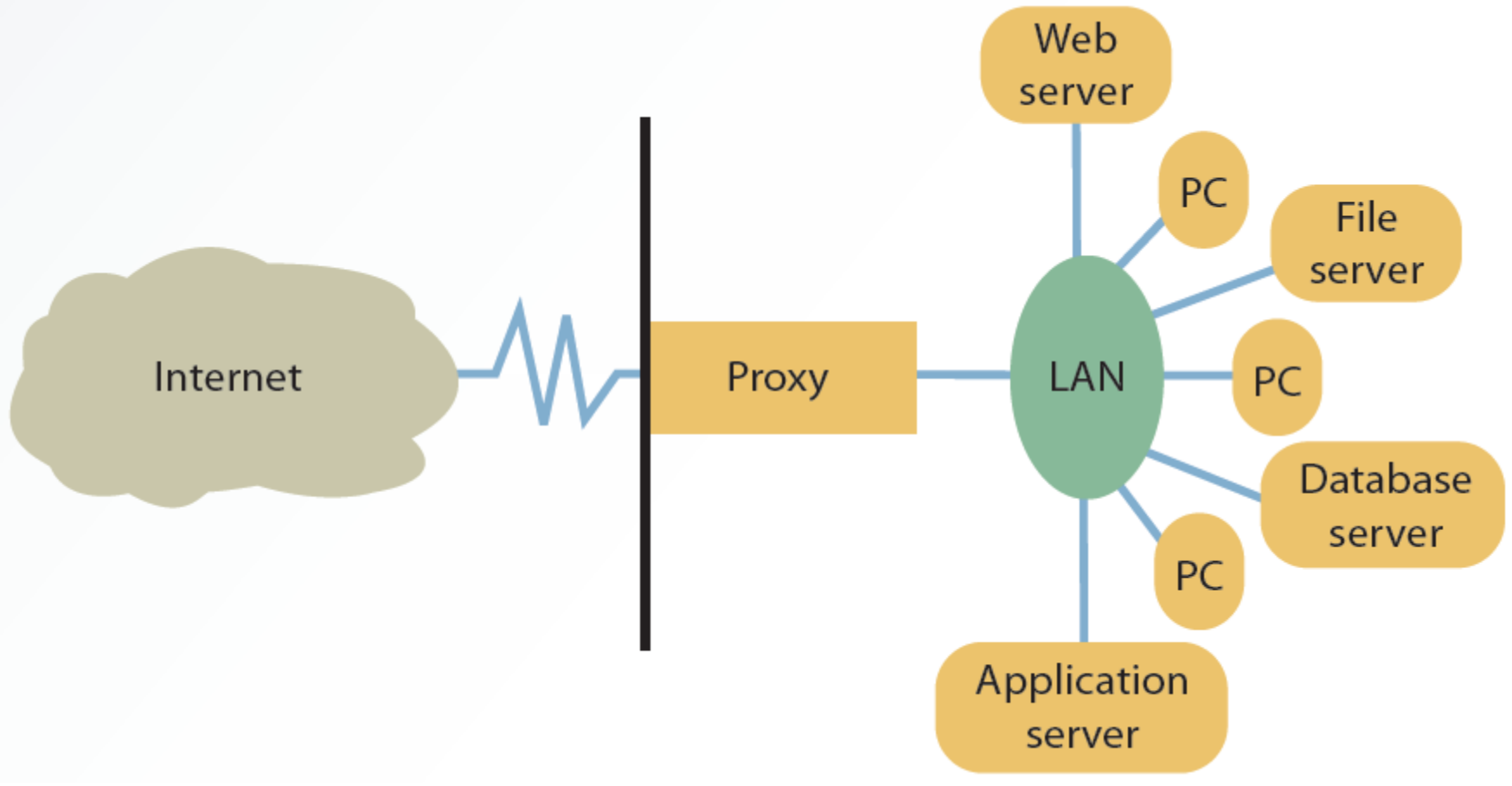
- Verify whether a user's access is valid
  - Done by logging the user off and then calling the user back at a predetermined number
  - Useful when many employees work off-site and need to connect to the network from remote locations

Firewalls

- Combinations of hardware and software that acts as a filter between a private network and external networks
  - Network administrator defines rules for access, and all other data transmissions are blocked
  - Types: packet-filtering firewalls, application-filtering firewalls, and proxy servers

Exhibit 5.3 Basic Firewall Configuration

Exhibit 5.4 Proxy Server



Intrusion Detection System (IDS)

- Protects against external and internal access
  - Placed in front of a firewall
  - Identifies attack signatures, traces patterns, and generates alarms for the network administrator
  - Causes routers to terminate connections with suspicious sources
  - Prevents DoS attacks

Physical Security Measures

- Control access to computers and networks
  - Include devices for securing computers and peripherals from theft
    - Cable shielding and room shielding
    - Corner bolts and steel encasements
    - Electronic trackers, identification (ID) badges, and proximity-release door openers

Access Controls

- Designed to protect systems from unauthorized access in order to preserve data integrity
  - Terminal resource security: erases the screen and signs the user off automatically after a specified length of inactivity
  - Passwords: combination of numbers, characters, and symbols that is entered to allow access to a system

Virtual Private Networks (1 of 2)

- Provides a secure tunnel through the Internet for transmitting messages and data via a private network
  - Gives remote users have a secure connection to the organization's network
  - Provides security for extranets

Virtual Private Networks (2 of 2)

- Data is encrypted before it is sent with a protocol
  - Layer Two Tunneling Protocol (L2TP)
  - Internet Protocol Security (IPSec)
- Advantage
  - Set-up costs are low
- Disadvantages
  - Slow transmission speed
  - Lack of standardization

Data Encryption (1 of 4)

- Transforms data, called plaintext or cleartext, into a scrambled form called ciphertext that cannot be read by others
  - Receiver unscrambles data using a decryption key
- Rules for encryption
  - Known as the encryption algorithm
  - Determine how simple or complex the transformation process should be

Data Encryption (2 of 4)

- Commonly used encryption protocols
  - Secure Sockets Layer (SSL)
    - Manages transmission security on the Internet
  - Transport Layer Security (TLS)
    - Cryptographic protocol that ensures data security and integrity over public networks, such as the Internet

Data Encryption (3 of 4)

- Asymmetric encryption uses two keys
  - Public key known to everyone
    - Encrypted message can be decrypted only with the same algorithm used by the public key and requires the recipient's private key
  - Private or secret key known only to the recipient
  - Drawback: slow and requires a large amount of processing power

Data Encryption (4 of 4)

- Symmetric (secret key) encryption: same key is used to encrypt and decrypt the message
  - Sender and receiver must agree on the key and keep it secret
  - Can be used to create digital signatures
  - Drawback: sharing the key over the Internet is difficult

E-Commerce Transaction Security Measures

- Concerned with several issues
  - Confidentiality
  - Authentication
  - Integrity
  - Nonrepudiation of origin
  - Nonrepudiation of receipt

Computer Emergency Response Team

- Developed by the Defense Advanced Research Projects Agency
  - Focuses on security breaches and DoS attacks
  - Offers guidelines on handling and preventing attacks
  - Conducts public awareness campaigns and researches Internet security vulnerabilities

Guidelines for a Comprehensive Security System (1 of 4)

- Before establishing a security program, organizations should:
  - Understand the principles of the Sarbanes-Oxley Act of 2002
  - Conduct a basic risk analysis, which makes use of financial and budgeting techniques
    - Information obtained helps organizations weigh the cost of a security system

Guidelines for a Comprehensive Security System (2 of 4)

- Steps when developing a comprehensive security plan
  - Set up a security committee
  - Post security policy in a visible place
  - Raise employee awareness
  - Use strong passwords
  - Install software patches and updates
  - Revoke terminated employees' passwords and ID badges immediately

Guidelines for a Comprehensive Security System (3 of 4)

- Keep sensitive data locked in secured locations
- Exit programs and systems promptly
- Limit computer access to authorized personnel only
- Compare communication logs with communication billings periodically
- Install antivirus programs, firewalls, and intrusion detection systems
- Use only licensed software

Guidelines for a Comprehensive Security System (4 of 4)

- Ensure fire protection systems and alarms are up to date, and test them regularly
- Check environmental factors
  - Temperature and humidity levels
- Use physical security measures
  - Corner bolts on workstations, ID badges, and door locks

Business Continuity Planning (1 of 2)

- Outlines procedures for keeping a firm operational in the event of a natural disaster or network attack
  - Disaster recovery plan lists the tasks that must be performed to restore damaged data and equipment and steps to prepare for disaster

Business Continuity Planning (2 of 2)

- Steps to follow when disaster strikes
  - Put together a management crisis team
  - Contact the insurance company
  - Restore phone communication systems
  - Notify all affected people that recovery is underway
  - Set up a help desk to assist affected people
  - Document all actions taken

Summary (1 of 2)

- Risks associated with information technologies can be minimized by:
  - Installing operating system updates regularly
  - Using antivirus/antispyware software and e-mail security features
- Comprehensive security system protects an organization's resources
  - Including information, computers, and network equipment

Summary (2 of 2)

- Network security threats can be categorized
  - Unintentional: natural disasters, accidental deletion of data, and structural failures
  - Intentional: hacker attacks and attacks by disgruntled employees
- Organizations must employ a variety of comprehensive security measures to guard against threats