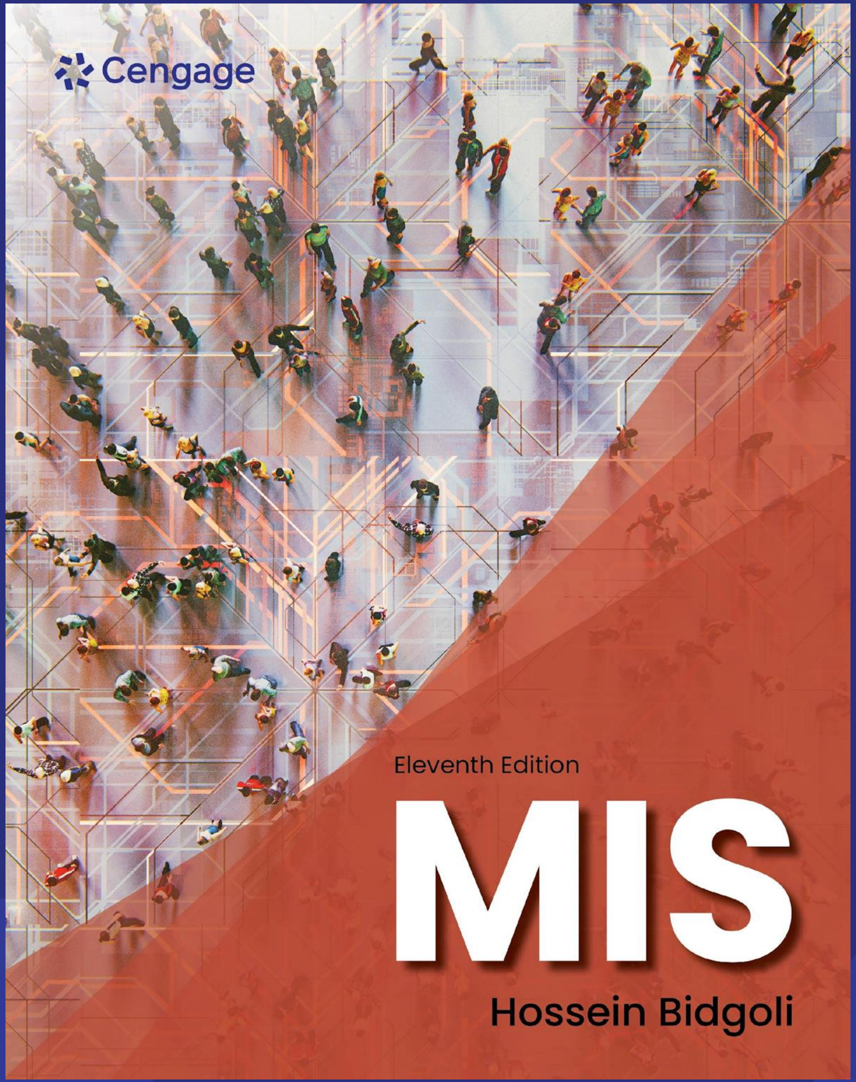


MIS, 11e

Module 5: Protecting Information Resources

Cengage

Module Objectives

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

- 5.1 Explain cybercrime and its impact on the global economy.
- 5.2 Describe information technologies that could be used in computer crimes.
- 5.3 Describe basic safeguards in computer, network, and cyber security.
- 5.4 Identify the ten most common intentional security threats.
- 5.5 Describe the nine security measures and enforcement that a comprehensive security system should include.
- 5.6 Summarize the guidelines for a comprehensive security system, including business continuity planning.

The Costs of Cyber Crime to the Global Economy

- According to Cybersecurity Ventures in 2020, cybercrime will cost the world economy $10.5 trillion annually by 2025.
- Costs include:
  - Loss of revenue
  - Stolen identities, intellectual property, and trade secrets
  - Damage to companies’ and individuals’ reputations
  - Expense of enhancing and upgrading a company’s cyber security
  - Loss of business information

Spyware and Adware

Spyware – Software gathers information about users while connected to the Internet.

- Some can change computer settings
- Prevent by installing antivirus or antispyware software

Adware – Form of spyware that collects information about the user to determine advertisements to display

- Prevent by installing an ad-blocking feature in the Web browser

Phishing, Pharming, Baiting, Quid Pro Quo, SMiShing, and Vishing

Phishing – Sending fraudulent e-mails that seem to come from legitimate sources (i.e., bank or university)

- Spear phishing – same as phishing by is target to a person or group

Pharming – Like phishing but the official Web site of an organization is hijacked by altering Web site IP address via a domain name system server

Baiting – Similar to phishing attacks but baiter gives recipient a promise (i.e., free software or gift card)
Quid pro quo – similar to baiting but Involves a hacker requesting the exchange of critical data or login information in exchange for a service or prize

SMiShing (SMS phishing) - technique that tricks user to download malware onto a mobile device

Vishing (voice or VoIP phishing) - **u**sing voice technology that tricks user into revealing important financial or personal information to unauthorized entities

Keystroke Loggers - Software or hardware devices that monitor and record keystrokes

Sniffing – capture and record network traffic

- Used by hackers to intercept information

Spoofing – attempt to gain access to a network by posing as an authorized user

- Used to find sensitive information
- Also happens when an illegitimate program poses as a legitimate one

Computer Crime and Fraud

Computer fraud – unauthorized use of computer data for personal gain

Computer crimes can include:

- Denial-of-service attacks
- Identity theft
- Software piracy, infringements of intellectual property
- Writing or spreading viruses, worms, Trojans and other malicious code
- Sabotage

Security Threats: An Overview (1 of 6)

- **Watch : https://www.youtube.com/watch?v=n8mbzU0X2nQ**
- **Viruses** – a self-propagating program code that is triggered by a specified time or event
  - Attaches to other files continuously
  - Transmitted through the network, e-mail, or message boards
- **Worms** – Independent programs that can spread without attaching to a host program
  - Eats up computing resources
  - Does not usually erase data

Security Threats: An Overview (2 of 6)

- **Trojan Programs** – Contain code intended to disrupt a computer, network, or Web site
  - Hidden inside a popular program
  - Can erase data
  - Do not replicate
- **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

Security Threats: An Overview (3 of 6)

- **Backdoors (or trapdoor)** – Programming routine built into a system
  - Enables the designer or programmer to bypass security at a later time
- **Blended threats** - Combines characteristics of viruses, worms, and malicious codes with vulnerabilities on networks
  - Searches for vulnerabilities and takes advantage of them
    - Embedding malicious codes in the server's HTML files
    - Sending unauthorized e-mails from compromised servers with a worm attachment

Security Threats: An Overview (4 of 6)

- **Rootkits** – Series of software tools that enable unauthorized access to computer or network system
  - Conceal their presence and actions
  - Can remotely execute files
  - Can change system configurations

Security Threats: An Overview (5 of 6)

- **Denial-of-service (DoS) attack** – 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 flood a Web site to cause it fail.
- **Botnet** - Network of computers and IoT devices infected with malicious software and controlled as a group.
- **TDoS (telephony denial of service) attacks** - High volumes of automated calls flood a target phone system, halting incoming and outgoing calls.

Security Threats: An Overview (6 of 6)

- **Social Engineering** – Using "people skills" to trick others into revealing private information.
  - Common techniques: dumpster diving, shoulder surfing, tailgating, scareware, pretexting
- **Cryptojacking** - Hackers secretly use victim’s computer to mine cryptocurrency.
  - Reduces performance of victim’s computer

Computer and Network Security: Basic Safeguards (1 of 3)

Comprehensive security system protects an organization’s resources

Three Levels of securities should be provided:

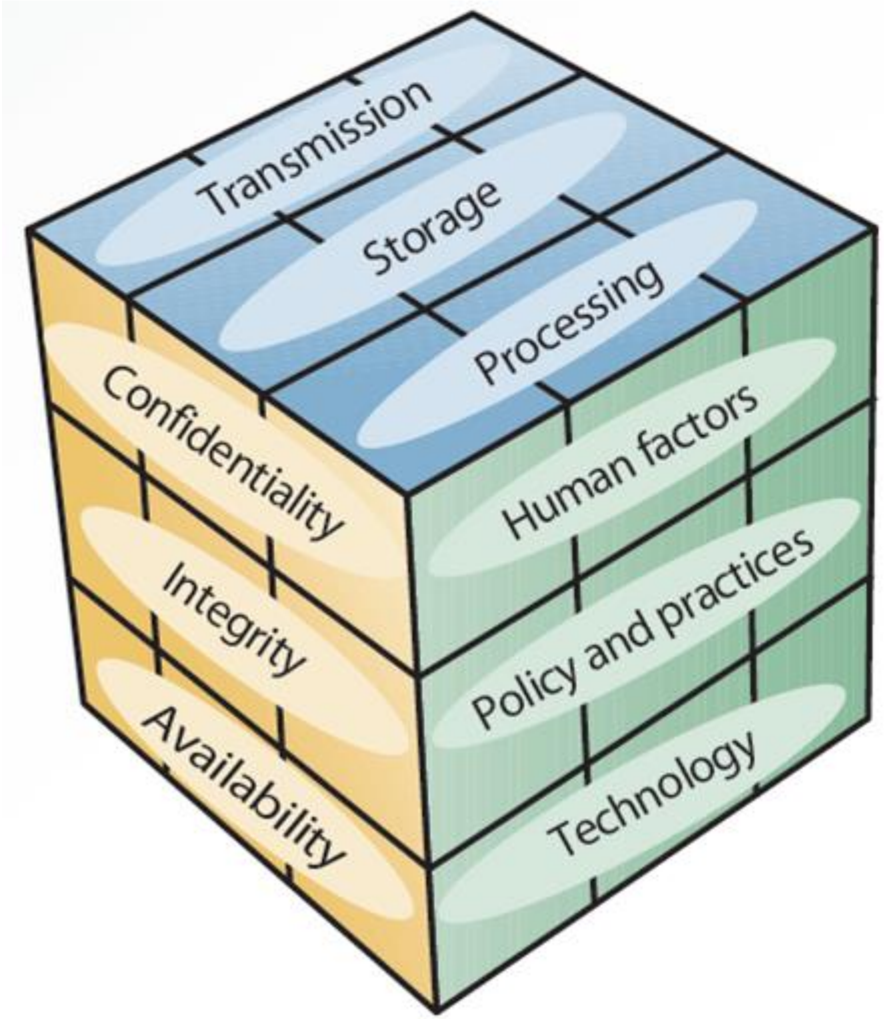
- Level 1: Front-end servers (e-mail and Web servers)
  - Protected against unauthorized access
- Level 2: Back-end systems (workstations and internal servers)
  - Protected to ensure data confidentiality, accuracy, and integrity
- Level 3: Corporate network
  - Protected against intrusion, denial-of-service attacks, and unauthorized access

Computer and Network Security: Basic Safeguards (2 of 3)

C-I-A triangle – important aspects of computer and network security

- **Confidentiality**
  - Information disclosed to authorized users only
- **Integrity**
  - Accuracy of information resources
- **Availability**
  - Computers and networks are operating; information accessible
  - Quick recovery from system failure or disaster

Exhibit 5.1 McCumber Cube



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

Planning a comprehensive security system: design fault-tolerant systems

- Ensure availability in the event of system failure using a combination of hardware and software
- Commonly used methods
  - Uninterruptible power supply (UPS)
    - https://www.youtube.com/watch?v=SsnORg72-d0
  - Redundant array of independent disks (RAID)
    - https://www.youtube.com/watch?v=U-OCdTeZLac
  - Mirror disks (= RAID-1)

Knowledge Check Activity 5-1

The first level of network security involves which of the following?

a. Public web server

b. Workstation

c. Corporate network

d. Intranet server

Knowledge Check Activity 5-1: Answer

The first level of network security involves which of the following?

Answer: a. Public web server

The first level of network security involves front-end servers like e-mail and web servers that are public facing or accessible via the Internet.

Security Measures and Enforcement: An Overview

A comprehensive security system should include:

- Biometric, nonbiometric, and physical security measures
- Access controls
- Virtual private networks
- Data encryption
- E-commerce transaction security measures
- Computer Emergency Response Team (CERT)
- Zero trust security

Biometric Security Measures

- Use a physiological element unique to a person that cannot be stolen, lost, copied, or passed on to others
  - Some biometric devices and measures: facial recognition, fingerprints, iris analysis, signature analysis, voice recognition
  - Some applications of biometrics:
    - ATM, credit and debit cards
    - Computer login security
    - Airport security and check-in

Nonbiometric Security Measures

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

Callback Modems

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

Firewalls

- Combinations of hardware and software that act as filters between private networks and external networks
  - Network administrator defines rules for access, and all other data transmissions are blocked
  - Types:
    - Packet-filtering firewalls
    - Application-filtering firewalls
      - https://www.youtube.com/watch?v=kDEX1HXybrU
    - Proxy servers
      - https://www.youtube.com/watch?v=5cPIukqXe5w

Exhibit 5.3 Basic Firewall Configuration

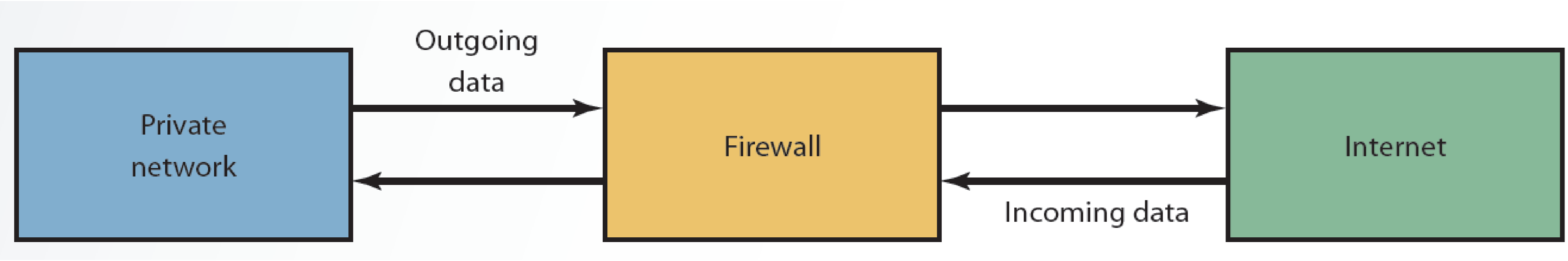
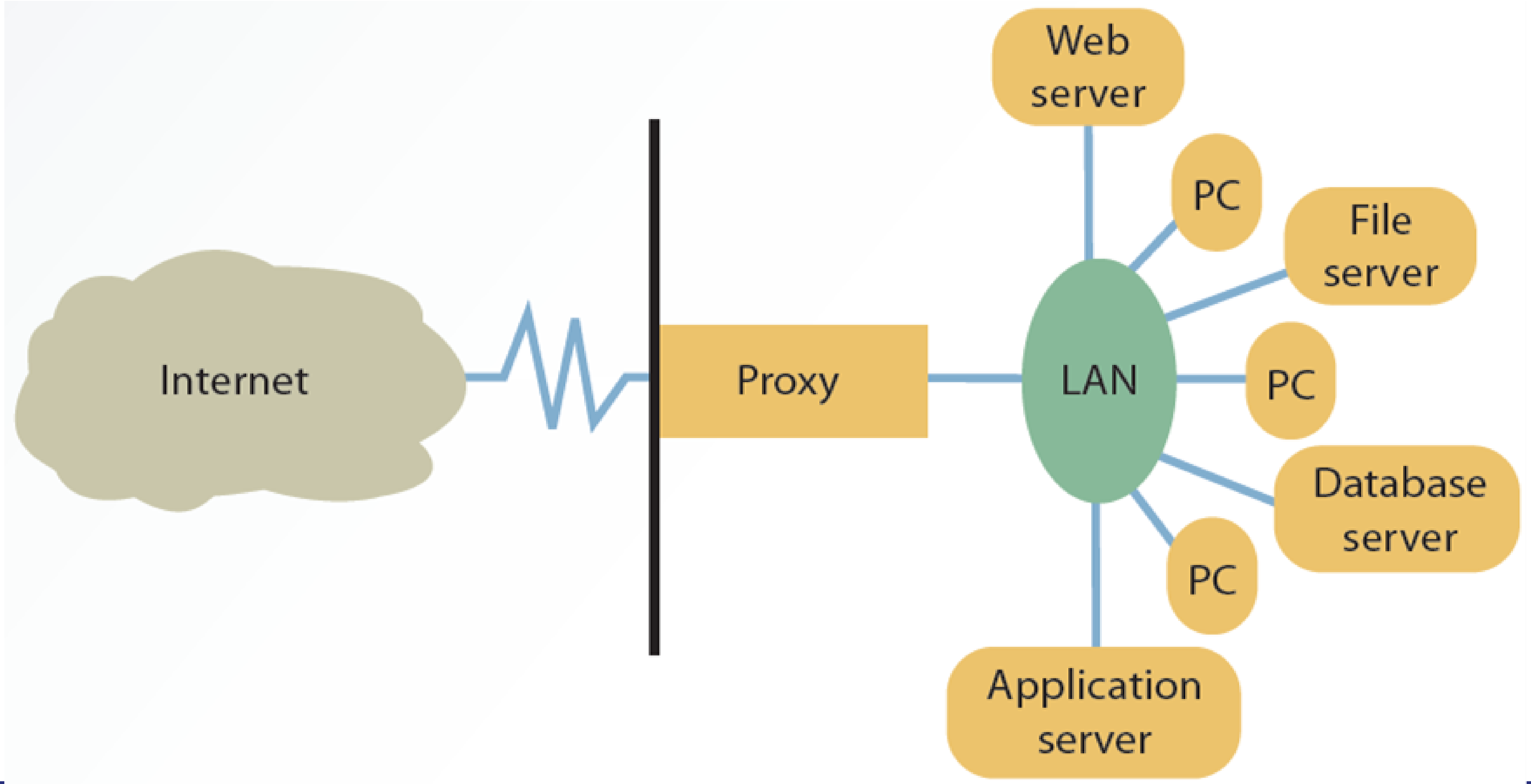


Exhibit 5.4 Proxy Server



Intrusion Detection System (IDS)

- Protects against both 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

Watch https://www.youtube.com/watch?v=_gHMkEKGwBM

Physical Security Measures

- Control access to computers and networks
  - Include devices for securing computers and peripherals from theft
    - Cable and room shielding
    - Corner bolts and steel encasements
    - Electronic trackers
    - Identification (ID) badges
    - Proximity-release door openers
    - Laptop cable locks

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:
    - Combinations of numbers, characters, and symbols that are entered to allow access to a system

- Password Manager - generates secure, random passwords for you and remembers them
  - Can sync with other devices (e.g., tablets, smartphones)
  - Encrypts your password database
- Other techniques to replace passwords: zero login, brain password, DNA identification, authentication tokens, and implanted microships

Virtual Private Networks

- Watch Video: https://www.youtube.com/watch?v=_wQTRMBAvzg
- Provides a secure tunnel through the Internet for transmitting messages and data
- Transmitted data is encrypted using L2TP and IPSec
- Advantage
  - Set-up costs are low
- Disadvantages
  - Slow transmission speed
  - Lack of standardization

Data Encryption (1 of 3)

- Watch Video： https://www.youtube.com/watch?v=jhXCTbFnK8o
- Transforms plaintext data into a scrambled form called ciphertext that cannot be read by others
  - Receiver unscrambles data using a decryption key
- Encryption algorithm determines how simple or complex the transformation process should be
  - Commonly used encryption protocols
  - https://www.youtube.com/watch?v=j9QmMEWmcfo
    - Secure Sockets Layer (SSL)
    - Transport Layer Security (TLS)

Data Encryption (2 of 3)

- Public key infrastructure (PKI)
  - Enables users of a public network (Internet) to exchange data
    - Secure and private
  - Uses a pair of keys obtained from a trusted authority:
    - Public key
    - Private key

Data Encryption (3 of 3)

- Asymmetric encryption uses two keys
  - Public key known to everyone
  - Private or secret key known only to the recipient
- 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

E-Commerce Transaction Security Measures

- Concerned with several issues
  - Confidentiality
  - Authentication
  - Integrity
  - Nonrepudiation of origin
    - Sender cannot deny having sent the data
  - Nonrepudiation of receipt
    - Recipient cannot deny having received the data

Zero Trust Security

- Requires every person and every device that accesses a network to be secure; inside or outside the organization.
- Main principles:
  - Every person or device must be verified
  - Least-privilege access
  - Microsegmentation
  - Multifactor authentication (MFA)

Knowledge Check Activity 5-2

Which is the most appropriate way to securely transmit data over the Internet?

a. Use a private key

b. Use symmetric encryption

c. Use a public key infrastructure

d. Use a virtual private network

Knowledge Check Activity 5-2: Answer

Which is the most appropriate way to securely transmit data over the Internet?

Answer: d. Use a virtual private network

A virtual private network (VPN) provides a secure tunnel through the Internet for transmitting messages and data using L2TP and IPSec.

Guidelines for a Comprehensive Security System (1 of 3)

Steps when developing a comprehensive security plan:

1. Set up a security committee
2. Post security policy in visible places
3. Raise employee awareness
4. Use strong passwords
5. Install software patches and updates
6. Revoke terminated employees’ passwords and ID badges immediately

Guidelines for a Comprehensive Security System (2 of 3)

Steps when developing a comprehensive security plan (continued):

7. Keep sensitive data, software, and printouts locked in secured locations
8. Exit programs and systems promptly
9. Limit computer access to authorized personnel only
10. Compare communication logs with communication billing
11. Install antivirus programs, firewalls, and intrusion detection systems
12. Use only licensed software

Guidelines for a Comprehensive Security System (3 of 3)

Steps when developing a comprehensive security plan (continued):

13. Ensure fire protection systems and alarms are up to date, and test them regularly
14. Check environmental factors
15. Use physical security measures
16. Install firewalls and IDS
17. Before recycle or donate, wipe data
18. Implement zero trust security

Business Continuity Planning (1 of 3)

- Outlines procedures for keeping an organization operational in the event of a natural disaster or network attack
- Tasks to prepare for and restore data:
  - Back up files
  - Periodically review security and fire standards for facilities
  - Periodically review information from CERT
  - Train staff members
  - Test plan with trial data

Business Continuity Planning (2 of 3)

- Tasks to prepare for and restore data (continued):
  - Identify vendors of all software and hardware
  - Document changes to hardware and software
  - Review insurance policies
  - Set up alternative sites
  - Keep backups off-site
  - Keep copy of disaster recovery plan off-site
  - Go through mock disaster to assess response

Business Continuity Planning (3 of 3)

Steps to resume normal operations when disaster strikes:

1. Put together a management crisis team
2. Contact the insurance company
3. Restore phone lines and other communication systems
4. Notify all affected people that recovery is underway
5. Set up a help desk to assist affected people
6. Document all actions taken

Self Assessment

Does your workplace or institution use a proxy server? And if so, what is its purpose?

What changes can you implement to make your current environment zero-trust?

Which part of developing a comprehensive security plan for a system would be most difficult for you personal?

Summary

Now that the lesson has ended, you should be able to:

- 5.1 Explain cybercrime and its impact on the global economy.
- 5.2 Describe information technologies that could be used in computer crimes.
- 5.3 Describe basic safeguards in computer, network, and cyber security.
- 5.4 Identify the ten most common intentional security threats.
- 5.5 Describe the nine security measures and enforcement that a comprehensive security system should include.
- 5.6 Summarize the guidelines for a comprehensive security system, including business continuity planning.