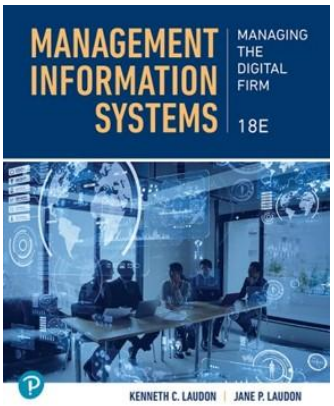
Management Information Systems: Managing the Digital Firm

Eighteenth Edition



Chapter 8

Securing Information Systems

Learning Objectives (1 of 2)

8.1 Understand why information systems are vulnerable.

8.2 Describe the most prevalent and dangerous types of malware.

8.3 Understand the dangers posed by threat actors.

8.4 Describe the security issues raised by software vulnerabilities.

8.5 Describe the security issues raised by artificial intelligence.

Learning Objectives (2 of 2)

8.6 Describe the business value of security and control.

8.7 Describe an organizational framework for security and control.

8.8 Discuss technologies for safeguarding information resources.

8.9 Understand how the information in this chapter can help your career.

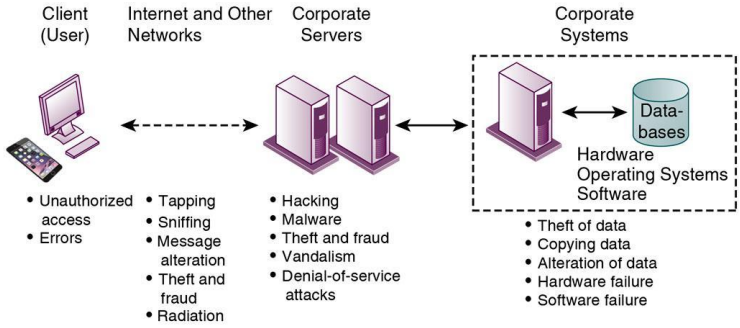
Understand Why Information Systems Are Vulnerable (1 of 3)

- if you operate a business today, you need to make security and control top priorities
  - Security
    - Policies, procedures, and technical measures used to prevent unauthorized access, alteration, theft, or physical damage to information systems
  - Controls
    - Methods, policies, and organizational procedures that ensure safety of organization's assets; accuracy and reliability of its accounting records; and operational adherence to management standards

Understand Why Information Systems Are Vulnerable (2 of 3)

- Threats can stem from technical, organizational, and environmental factors and be compounded by poor management decisions
  - Threat actor
    - An individual or group of individuals seeking to exploit system vulnerabilities to intentionally cause harm
  - System malfunctions
  - Domestic or offshore partnering can lead to vulnerability
  - Portability
  - Vulnerability

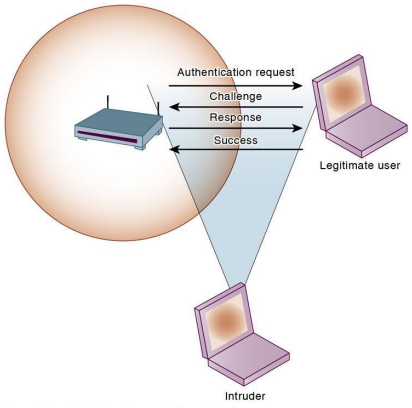
Figure 8.1 Contemporary Security Challenges and Vulnerabilities



Understand Why Information Systems Are Vulnerable (3 of 3)

- Sniffer
  - A type of eavesdropping program that monitors information traveling over a network
- Both Bluetooth and Wi-Fi networks are susceptible to hacking by eavesdroppers
  - Wardriving
    - Eavesdroppers drive by buildings or park and try to intercept wireless network traffic
  - Rogue access points

Figure 8.2 Wi-Fi Security Challenges



Describe the Most Prevalent and Dangerous Types of Malware (1 of 2)

- Malware (malicious software programs)
- Variety of threats
  - Viruses
  - Worms
  - Trojan horses
  - Ransomeware
  - Bot
    - Botnet

Describe the Most Prevalent and Dangerous Types of Malware (2 of 2)

- Potentially unwanted programs (PUPs)
- Drive-by download
- Malvertising
- Keylogger

Understand the Dangers Posted by Threat Actors (1 of 3)

- There are numerous types of threat actors
  - Cybercriminals
  - Hackers
    - Ethical hackers
  - Hacktivists
    - Often engage in cybervandalism

Understand the Dangers Posted by Threat Actors (2 of 5)

- Threat actors often employ
  - Spoofing
    - The practice of tricking or deceiving others by hiding one's true identity

Understand the Dangers Posted by Threat Actors (3 of 5)

- One popular form of spoofing is
  - Phishing
    - Involves setting up fake websites or sending email messages that look like those of legitimate businesses to ask users for confidential personal data
  - Phishing often involves
    - Social engineering
    - Evil twin
    - Pharming

Understand the Dangers Posted by Threat Actors (4 of 5)

- One popular form of spoofing is
  - Phishing
    - Involves setting up fake websites or sending email messages that look like those of legitimate businesses to ask users for confidential personal data
  - Phishing often involves
    - Social engineering
    - Evil twin
    - Pharming

Understand the Dangers Posted by Threat Actors (5 of 5)

- Advanced persistent attacks
  - Living off the Land attack (LOTL attack)
    - Often referred to as a “fileless” attack
  - Advanced persistent threat attack (APT attack)
    - Prolonged attack where an intruder infiltrates the system and remains undetected for an extended period of time
  - Denial-of-service attack (DoS attack)
    - Attackers flood a network or web server with thousands of false communications or service requests in order to crash the network
  - Distributed denial-of-service attack (DDoS attack)
    - Often employs a botnet to inundate and overwhelm a network

Data Breaches and Identity Theft

- Data breach
- Credential stuffing attack
- Identity theft

Global Threats

- Cyberwarfare
  - State-sponsored politically motivated activity designed to harm another state or nation
- Cyberterrorism
  - Executed by a terrorist group

Internal Threats: Employees

- Security threats often originate inside an organization
- Inside knowledge
- Sloppy security procedures
  - User lack of knowledge
- Social engineering
- Both end users and information systems specialists are sources of risk

Computer Crime (1 of 2)

- Computer crime defined by U.S. Department of Justice as any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution.
- Computer may be target of crime
- Computer may be instrument of crime

Computer Crime (2 of 2)

There are numerous state and federal laws to try to prevent or reduce computer crime.

No one knows the magnitude of computer crime—how many systems are invaded, how many people engage in the practice, or the total economic damage that results from computer crime.

The estimated global cost of cybercrime in 2024 will be $9.5 trillion.

Describe the Security Issues Raised by Software Vulnerabilities (1 of 2)

- Commercial software contains flaws that create security vulnerabilities
  - Bugs (program code defects)
  - Zero defects cannot be achieved
  - Flaws can open networks to intruders
- Zero-day vulnerability

Describe the Security Issues Raised by Software Vulnerabilities (2 of 2)

- SQL injection attack
- Patch
  - Patch management
- Software supply chain attack

Describe the Security Issues Raised by Artificial Intelligence

In addition to the benefits of AI, there are also some significant challenges and risks in terms of cybersecurity

- Phishing with AI
- Deepfakes
- Subverting LLMs

Describe the Security Issues Raised by Software Vulnerabilities (1 of 3)

- Failed computer systems can lead to significant or total loss of business function
- A security breach may cut into a firm's market value almost immediately
- Inadequate security and control may result in serious legal liability

Describe the Security Issues Raised by Software Vulnerabilities (2 of 3)

- Electronic records management (ERM)
- Health Insurance Portability and Accountability Act (HIPAA)
  - Medical security and privacy rules and procedures
- Gramm-Leach-Bliley Act
  - Requires financial institutions to ensure the security and confidentiality of customer data
- Sarbanes-Oxley Act
  - Imposes responsibility on companies and their management to safeguard the accuracy and integrity of financial information that is used internally and released externally

Describe the Security Issues Raised by Software Vulnerabilities (3 of 3)

- Electronic evidence
  - Evidence for white collar crimes often in digital form
  - Proper control of data can save time and money when responding to legal discovery request
- Digital forensics
  - Scientific collection, examination, authentication, preservation, and analysis of data from computer storage media for use as evidence in court of law
  - Recovery of ambient data

Describe an Organizational Framework for Security and Control

- Need to develop a security policy
  - May be automated or manual
- General controls
  - Govern design, security, and use of computer programs and security of data files in general throughout organization
- Application controls
  - Controls unique to each computerized application
  - Input controls, processing controls, output controls

Risk Assessment

- Determines level of risk to firm if specific activity or process is not properly controlled
  - Types of threat
  - Probability of occurrence during year
  - Potential losses, value of threat
  - Expected annual loss

Risk assessment determines the level of risk to a firm if a specific activity or process is not properly controlled.

Table 8.5 Online Order Processing Risk Assessment

Exposure	Probability of Occurrence (%)	Loss Range/Average ($)	Expected Annual Loss ($)
Power failure	30%	$5,000–$200,000 ($102,500)	$30,750
Embezzlement	5%	$1,000–$50,000 ($25,500)	$1,275
User error	98%	$200–$40,000 ($20,100)	$19,698

Security Policy

- Security policy
  - Consists of statements ranking information risks, identifying acceptable security goals, and identifying the mechanisms for achieving these goals
  - Drives other policies
- Acceptable use policy (A U P)
  - Defines acceptable uses of firm's information resources and computing equipment

Disaster Recovery Planning and Business Continuity Planning

- Disaster recovery planning
  - Devises plans for restoration of disrupted services
- Business continuity planning
  - Focuses on restoring business operations after disaster
- Both types of plans needed to identify firm's most critical systems
  - Business impact analysis to determine impact of an outage
  - Management must determine which systems restored first

The Role of Auditing

- Information systems audit
  - Examines firm's overall security environment as well as controls governing individual information systems
- Security audits
  - Review technologies, procedures, documentation, training, and personnel
- List and rank control weaknesses and the probability of occurrence
- Assess financial and organizational impact of each threat

Discuss Technologies for Safeguarding Information Resources (1 of 4)

- Identity and access management software (IAM software)
  - Automates keeping track of all users and privileges
- Zero trust
  - Popular cybersecurity framework based on the principle of maintaining strict access controls

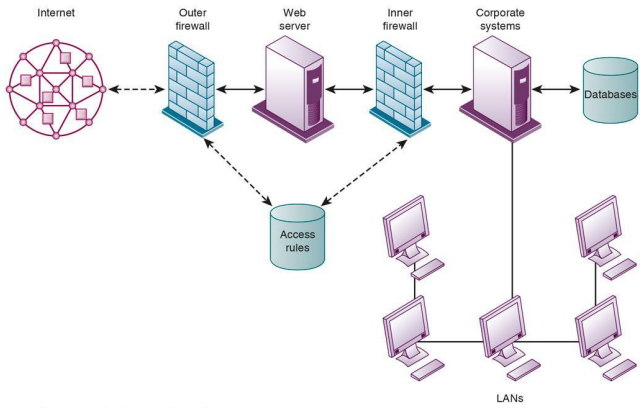
Discuss Technologies for Safeguarding Information Resources (2 of 4)

- Authentication
  - The ability to know that people are who they claim to be
    - Password
    - Token
    - Smart cards
    - Biometric authentication
    - Multifactor authentication
    - Two-factor authentication

Discuss Technologies for Safeguarding Information Resources (3 of 4)

- Firewall
  - Prevents unauthorized users from accessing private networks
  - Packet filtering
  - Stateful inspection
  - Network address translation (N A T)
  - Application gateways
  - Next-generation firewall (NGFW)

Figure 8.5 A Corporate Firewall



Discuss Technologies for Safeguarding Information Resources (4 of 4)

- Intrusion detection system
  - Monitors hot spots on corporate networks to detect and deter intruders
- Intrusion prevention system (IPS)
  - Additional ability to take steps to prevent and block suspicious activities
- Anti-malware software
  - Detects and eliminates malware
- Unified threat management (U T M) systems
  - Combines various security tools

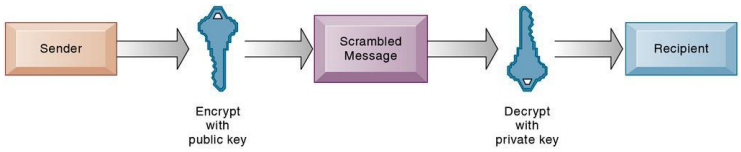
Securing Wireless Networks

- W E P
- W P A 2
- W P A3

Encryption and Public Key Infrastructure (1 of 2)

- Encryption
  - Process of transforming plain text or data into cipher text read only the sender and intended receiver
  - Transport Layer Security (TLS)
  - HTTPS
  - Public key encryption

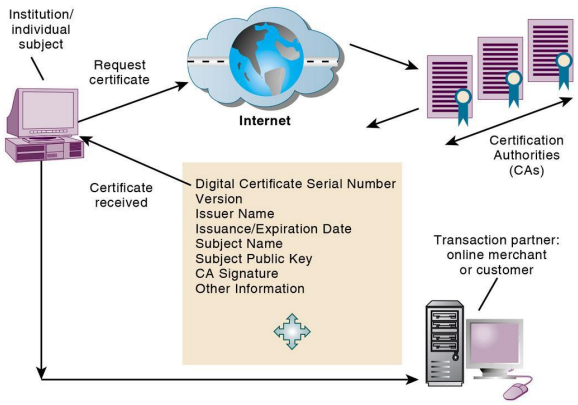
Figure 8.6 Public Key Encryption



Encryption and Public Key Infrastructure (2 of 2)

- Digital certificate
  - Data file used to establish the identity of users and electronic assets for protection of online transactions
- Public key infrastructure (P K I)
  - Use of public key cryptography working with certificate authority
  - Widely used in e-commerce

Figure 8.7 Digital Certificates



Securing Transactions with Blockchain

- A blockchain is a chain of digital "blocks" that contain records of transactions
  - Secure transaction database
  - Encryption used to verify users and transactions
  - Decentralized
  - Records cannot be changed
  - Blockchain has some vulnerabilities requiring attention to security and controls
  - Cryptocurrencies

Ensuring System Availability

- Online transaction processing requires 100% availability
- Fault-tolerant computer systems
  - Contain redundant hardware, software, and power supply components that create an environment that provides continuous, uninterrupted service
- Security operations center
- Managed security service providers (M S S P s)
- Digital resiliency

Security Issues for Cloud Computing and the Mobile Digital Platform (1 of 2)

- Security in the cloud
  - Responsibility for security resides with company owning the data
  - Firms must ensure providers provide adequate protection:
    - Where data are stored
    - Meeting corporate requirements, legal privacy laws
    - Segregation of data from other clients
    - Audits and security certifications
  - Service level agreements (S L A s)

Security Issues for Cloud Computing and the Mobile Digital Platform (2 of 2)

- Securing mobile platforms
  - Security policies should include and cover any special requirements for mobile devices
    - Guidelines for use of platforms and applications
  - Mobile device management (MDM)
    - Authorization
    - Inventory records
    - Control updates
    - Lock down/erase lost devices
    - Encryption
  - Software for segregating corporate data on devices

Ensuring Software Quality

- Software metrics: Objective assessments of system in form of quantified measurements
  - Number of transactions
  - Online response time
  - Payroll checks printed per hour
  - Known bugs per hundred lines of code
- Early and regular testing
- Walkthrough: Review of specification or design document by small group of qualified people
- Debugging: Process by which errors are eliminated

Copyright