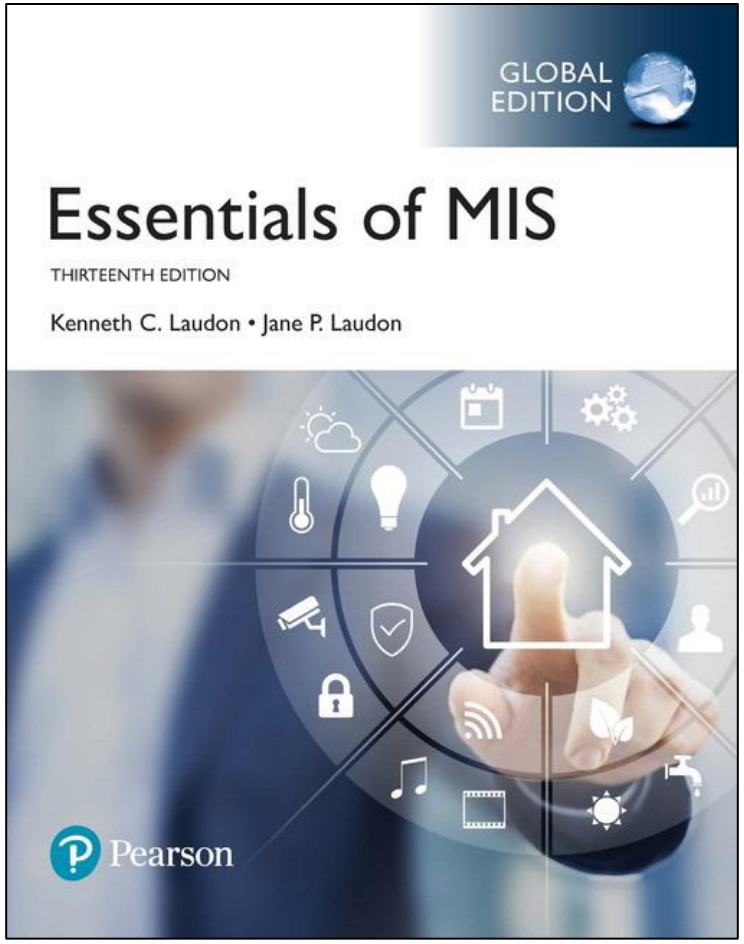
Essentials of Management Information Systems

Thirteenth Edition



Chapter 8

Securing Information Systems

Learning Objectives

8.1 Why are information systems vulnerable to destruction, error, and abuse?

8.2 What is the business value of security and control?

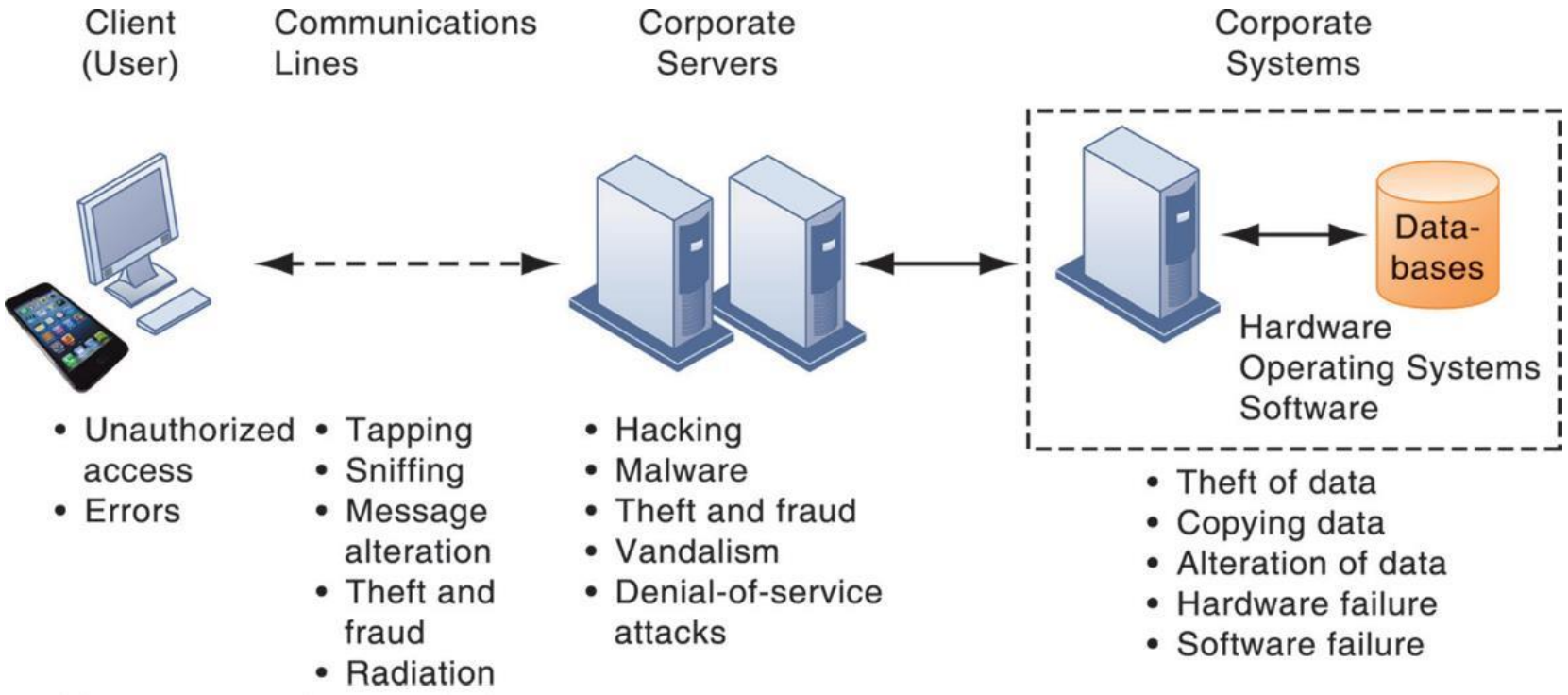
8.3 What are the components of an organizational framework for security and control?

8.4 What are the most important tools and technologies for safeguarding information resources?

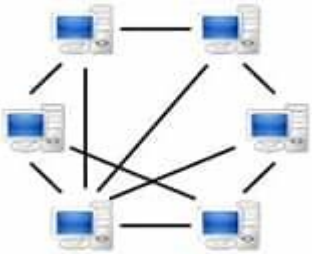
Why Systems are Vulnerable

- **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
- **Accessibility of networks**
- Hardware problems (breakdowns, configuration errors, damage from improper use or crime)
- Software problems (programming errors, installation errors, unauthorized changes)
- Disasters
- Use of networks/computers outside of firm's control
- Loss and theft of portable devices

Figure 8.1 Contemporary Security Challenges and Vulnerabilities

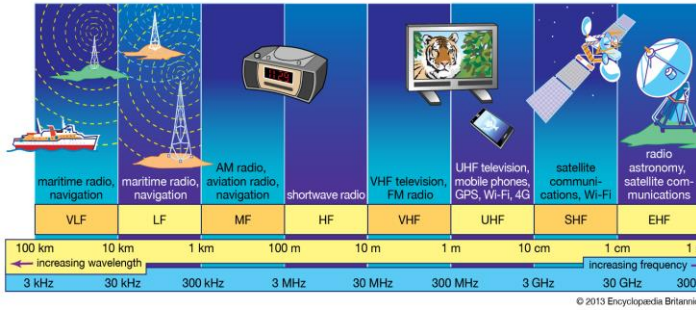


Internet Vulnerabilities



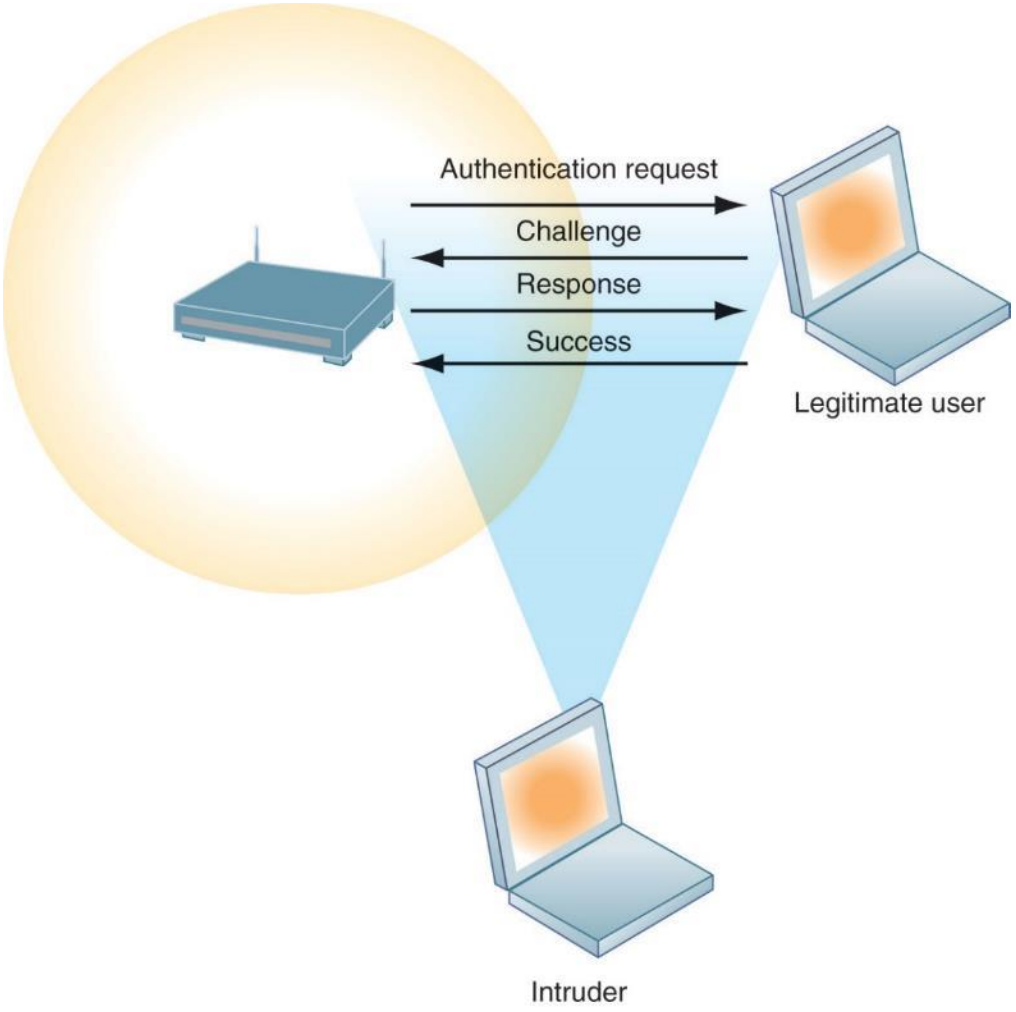
- Network open to anyone
- Size of Internet means abuses can have wide impact
- Use of fixed Internet addresses with cable / DSL modems creates fixed targets for hackers
- Unencrypted VOIP (Voice over Internet Protocol (VoIP), is a technology that allows you to make voice calls using a broadband Internet connection instead of a regular (or analog) phone line
- Email, P2P (Peer-to-peer computing or networking is a distributed application architecture that partitions tasks or workloads between peers. Peers are equally privileged, equipotent participants in the application.), IM. Internet Multimedia. Multimedia is a mixture of graphics, video, animation, audio, 3-D/ Virtual Reality and text. These are combined and conveyed interactively via electronic or digital means
  - Interception
  - Attachments with malicious software
  - Transmitting trade secrets

Wireless Security Challenges



- Radio frequency bands easy to scan
- SSIDs (service set identifiers) is a **sequence of characters that uniquely names a wireless local area network (WLAN)**. An SSID is sometimes referred to as a "network name." This name allows stations to connect to the desired network when multiple independent networks operate in the same physical area.
  - Identify access points, broadcast multiple times, can be identified by sniffer programs
- War driving
  - Eavesdroppers (Eavesdropping is the act of secretly or stealthily listening to the private conversation or communications of others without their consent in order to gather information.) drive by buildings and try to detect SSID and gain access to network and resources
  - Once access point is breached, intruder can gain access to networked drives and files
- Rogue access points

Figure 8.2 Wi-Fi Security Challenges



Malicious Software: Viruses, Worms, Trojan Horses, and Spyware (1 of 2)

- Malware (malicious software) Malware is any software intentionally designed to cause damage to a computer, server, client, or computer network. By contrast, software that causes unintentional harm due to some deficiency is typically described as a software bug. A wide variety of malware types exist, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, rogue software, wiper and scareware.

- Computer Viruse is a type of malicious code or program written to alter the way a computer operates and that is designed to spread from one computer to another. A virus operates by inserting or attaching itself to a legitimate program or document that supports macros in order to execute its code.

- Worms A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. It often uses a computer network to spread itself, relying on security failures on the target computer to access it. It will use this machine as a host to scan and infect other computers.

- **Worms and viruses spread by: (1)**Downloads and drive-by downloads (2) Mobile device malware

(3) Social network malware (4) Email, I M attachments

Malicious Software: Viruses, Worms, Trojan Horses, and Spyware (2 of 2)

- Trojan horse is a type of malicious code or software that looks legitimate but can take control of your computer. A Trojan is designed to damage, disrupt, steal, or in general inflict some other harmful action on your data or network.
- SQL injection attacks SQL is a code injection technique used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's
- Ransomware is a type of malware from cryptovirology that threatens to publish the victim's personal data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system so that it is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion.
- Spyware is software with malicious behavior that aims to gather information about a person or organization and send it to another entity in a way that harms the user. For example, by violating their privacy or endangering their device's security.
  - Key loggers
  - Other types
    (1) Reset browser home page
    (2) Redirect search requests
    (3) Slow computer performance by taking up memory

Hackers and Computer Crime (1 of 2)

- Hackers vs. Crackers A hacker is a computer expert that uses their technical knowledge to overcome a problem while **a cracker is a person who breaks into someone else's computer or a network illegally**. Thus, this is the fundamental difference between hacker and cracker.
- Activities include:
  - System intrusion
  - System damage
  - Cybervandalism
    - Intentional disruption, defacement, destruction of website or corporate information system
- Spoofing and sniffing
  - Sniffing is a passive security attack in which a machine separated from the intended destination reads data on a network. ... IP
- Spoofing is the technique used by intruders to gain access to a Network by sending messages to a computer with an IP address indicating that the message is coming from a trusted hostDenial-of-service attacks (DoS) is a Distributed
- **initially small queries into much larger payloads**, which are used to bring down the victim's serve
- Denial of Service (DDoS) attack **in which the attacker exploits vulnerabilities in domain name system (DNS) servers to turn**
- Distributed denial-of-service attacks (DDoS) attacks **target websites and online services**. The aim is to overwhelm them with more traffic than the server or network can accommodate. The goal is to render the website or service inoperable. ... In some cases, the targeted victims are threatened with a DDoS attack or attacked at a low level

Hackers and Computer Crime (2 of 2)

- Botnet is a form of malware that involves an inter-connected network of hacked computers that lead back to a centralized computer controlled by a cyber criminal, who can then easily deploy cyber attacks to the entire network

- Spam can be defined as **irrelevant or unsolicited messages sent over the Internet**. These are usually sent to a large number of users for a variety of use cases such as advertising, phishing, spreading malware, etc.

- Computer crime
  - Computer may be target of crime
  - Computer may be instrument of crime

- Identity theft
  - Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.
  - Evil twins is a rogue wireless access point that masquerades as a legitimate Wi-Fi access point so that an attacker can gather personal or corporate information without the end-user's knowledge.
  - Pharming vs Phishing What is the Difference Between Phishing and Pharming? ... While phishing attempts are carried out by using spoofed websites, appearing to have come from legitimate entities, pharming relies on the DNS server level. Unlike phishing, **pharming doesn't rely on bait** like fake links to trick users.

- Click fraud is the act of clicking on a paid link, such as display ad or sponsored search result, with malicious or vindictive intent. This can be to deplete the advertisers marketing budget, damage the performance or reach of the ad, or even to steal the cost of that click for yourself (a practice known as ad fraud

- Cyberterrorism is the use of the Internet to conduct violent acts that result in, or threaten, the loss of life or significant bodily harm, in order to achieve political or ideological gains through threat or intimidation.

- Cyberwarfare is the use of digital attacks to attack a nation, causing comparable harm to actual warfare and/or disrupting the vital computer systems. ... However, meeting the scale and protracted nature of war is unlikely, thus ambiguity remains

Internal Threats: Employees

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

Software Vulnerability

- Commercial software contains flaws that create security vulnerabilities
  - Bugs (program code defects)
  - Zero defects cannot be achieved n **larger software programs** because fully testing programs that contain thousands of choices and millions of paths would require thousands of years. An acceptable use policy defines the acceptable level of access to information assets for different users.
  - Flaws (Errors) can open networks to intruders
- Zero-day vulnerabilities
- Patches are small pieces of software to repair flaws (Errors)
  - Patch management is **the process of distributing and applying updates to software**. ... Common areas that will need patches include operating systems, applications, and embedded systems (like network equipment).

What is the Business Value of Security and Control?

- Failed computer systems can lead to significant or total loss of business function
- Firms now are more vulnerable than ever
  - Confidential personal and financial data
  - Trade secrets, new products, strategies
- A security breach may cut into a firm's market value almost immediately
- Inadequate security and controls also bring forth issues of liability

Legal and Regulatory Requirements for Electronic Records Management

- **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

Electronic Evidence and Computer Criminal

- 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
- Computer 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

Information Systems Controls

- May be automated or manual
- General controls
  - Govern design, security, and use of computer programs and security of data files in general throughout organization
  - Software controls, hardware controls, computer operations controls, data security controls, system development controls, administrative controls,
- 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

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 theft or misappropriation of funds placed in one's trust or belonging to one's employer.	5%	$1,000 − $50,000 ($25,500)	$1275
User error	98%	$200 − $40,000 ($20,100)	$19,698

Security Policy

- Ranks information risks, identifies security goals and mechanisms for achieving these goals
- Drives other policies
- Acceptable use policy (AUP)
  - Defines acceptable uses of firm's information resources and computing equipment.
  - It Includes **specific rules**, such as no video pirating. Outlines consequences for breaking the rules, such as warnings or suspension of access. Details an organization's philosophy for granting access (for example, internet use is a privilege that can be revoked, rather than a right)
- Identity management
  - Identifying valid users
  - Controlling access

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
  - May even simulate disaster to test responses
- List and rank control weaknesses and the probability of occurrence
- Assess financial and organizational impact of each threat

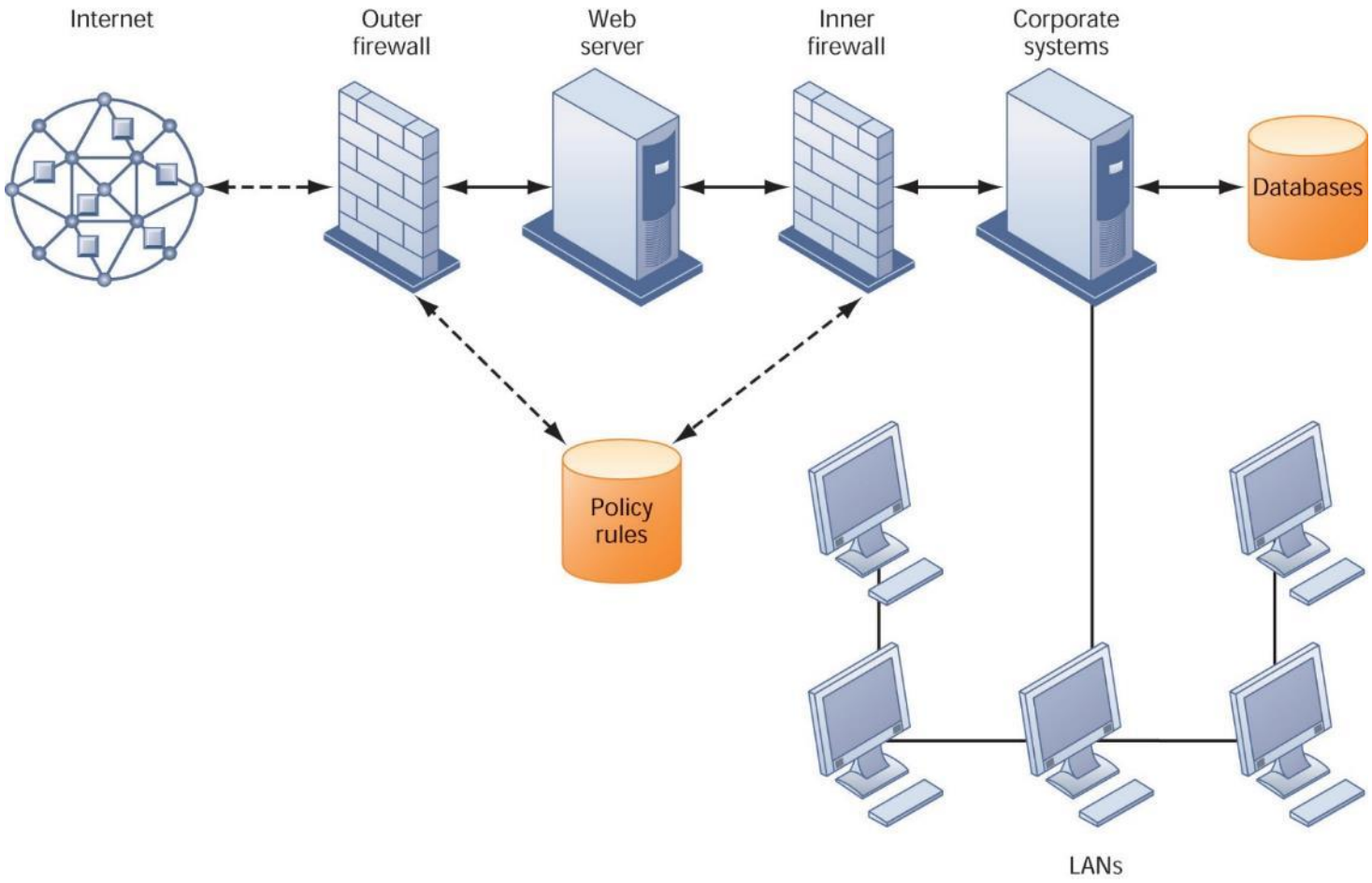
Figure 8.4 Sample Auditor's List of Control Weaknesses

Function: Loans **Location: Peoria, IL**	**Prepared by: J. Ericson** **Date: June 16, 2017**		**Received by: T. Benson** **Review date: June 28, 2017**	
Nature of Weakness and Impact	Chance for Error/Abuse		Notification to Management	
	Yes/ No	Justification	Report date	Management response
User accounts with missing passwords	Yes	Leaves system open to unauthorized outsiders or attackers	5/10/17	Eliminate accounts without passwords
Network configured to allow some sharing of system files	Yes	Exposes critical system files to hostile parties connected to the network	5/10/17	Ensure only required directories are shared and that they are protected with strong passwords
Software patches can update production programs without final approval from Standards and Controls group	No	All production programs require management approval; Standards and Controls group assigns such cases to a temporary production status		

Tools and Technologies for Safeguarding Information Systems (1 of 2)

- Identity management software
  - Automates keeping track of all users and privileges
  - Authenticates users, protecting identities, controlling access
- Authentication
  - Password systems
  - Tokens
  - Smart cards
  - Biometric authentication
  - Two-factor authentication
- Firewall
  - Combination of hardware and software that prevents unauthorized users from accessing private networks
  - Packet filtering
  - Stateful inspection
  - Network address translation (NAT)
  - Application proxy filtering

Figure 8.5 A Corporate Firewall



Tools and Technologies for Safeguarding Information Systems (2 of 2)

- Intrusion detection system
  - Monitors hot spots on corporate networks to detect and deter intruders
- Antivirus and antispyware software
  - Checks computers for presence of malware and can often eliminate it as well
  - Requires continual updating
- Unified threat management (UTM) systems

Securing Wireless Networks

- WEP security
  - Static encryption keys are relatively easy to crack
  - Improved if used in conjunction with VPN
- WPA2 specification
  - Replaces WEP with stronger standards
  - Continually changing, longer encryption keys

Encryption and Public Key Infrastructure (1 of 2)

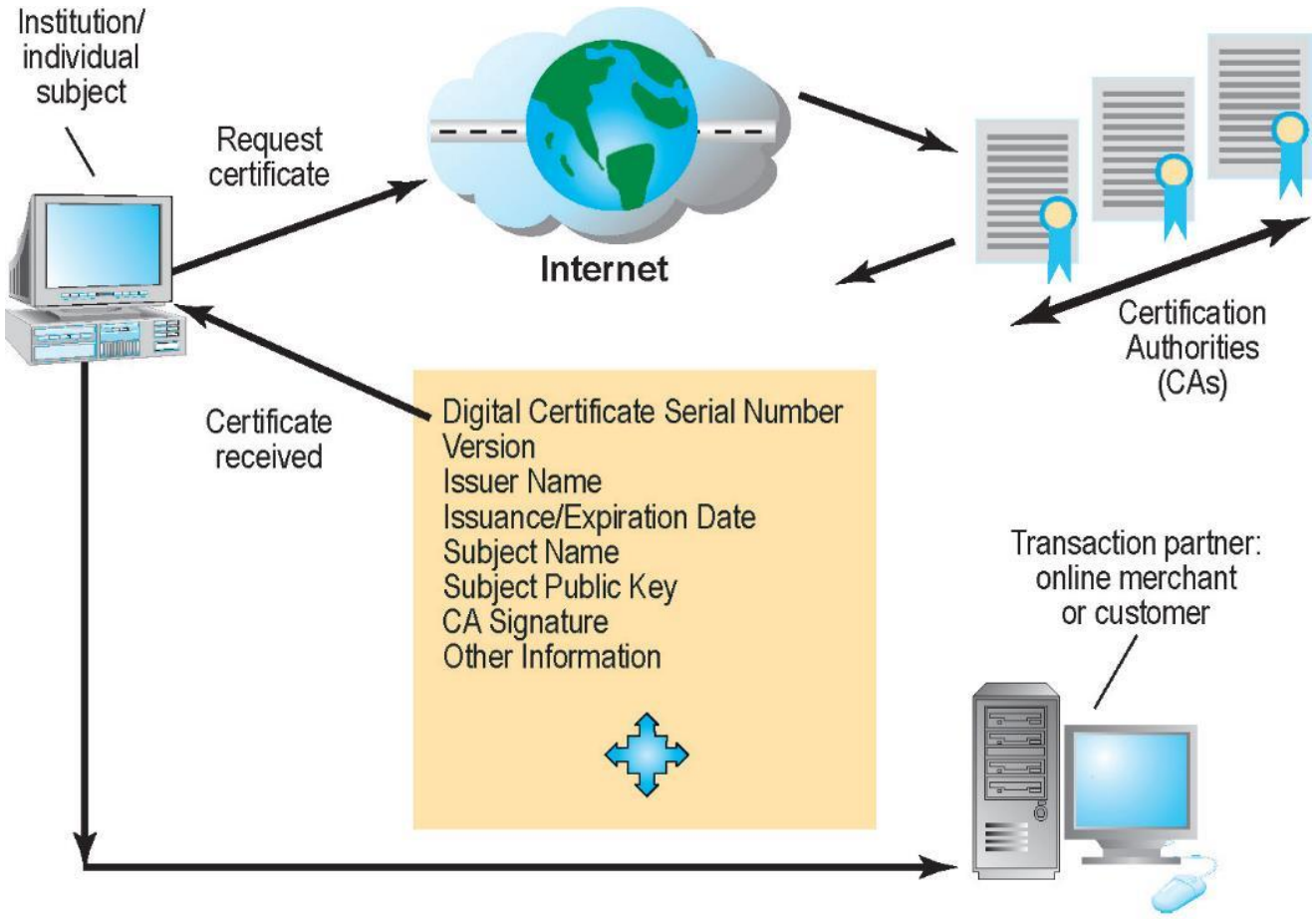
- Encryption
  - Transforming text or data into cipher text that cannot be read by unintended recipients
  - Two methods for encryption on networks
    - Secure Sockets Layer (SSL) and successor Transport Layer Security (TLS)
    - Secure Hypertext Transfer Protocol (S-HTTP)
- Two methods of encryption of messages
  - Symmetric key encryption
    - Sender and receiver use single, shared key
  - Public key encryption
    - Uses two, mathematically related keys: public key and private key
    - Sender encrypts message with recipient's public key
    - Recipient decrypts with private key

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
  - Uses a trusted third party, certification authority (CA), to validate a user's identity
  - CA verifies user's identity, stores information in CA server, which generates encrypted digital certificate containing owner ID information and copy of owner's public key
- Public key infrastructure (PKI)
  - Use of public key cryptography working with certificate authority
  - Widely used in e-commerce

Figure 8.7 Digital Certificates



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
- Deep packet inspection
- Security outsourcing
  - Managed security service providers (MSSPs)

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 (SLAs)

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 tools
    - 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

Interactive Session: Organizations: How Secure is BYOD?

- BYOD stands for bring your own device. It's an IT policy that allows, and sometimes encourages, employees to access enterprise data and systems using personal mobile devices such as smartphones, tablets and laptops. There are four basic options or access levels to BYOD: Access, but preventing local storage of data on personal devices

- Class discussion **Bonus**
  - It has been said that a smartphone is a computer in your hand. Discuss the security implications of this statement.
  - What kinds of security problems do mobile computing devices pose?
  - What management, organizational, and technology issues must be addressed by smartphone security?
  - What steps can individuals and businesses take to make their smartphones more secure?