Chapter 8

Securing Information Systems

STUDENT LEARNING OBJECTIVES

- Why are information systems vulnerable to destruction, error, and abuse?
- What is the business value of security and control?
- What are the components of an organizational framework for security and control?
- What are the important tools and technologies for safeguarding information resources?

Student Support Materials

Learning Tracks

1. The Booming Job Market in IT Security
2. The Sarbanes Oxley Act
3. Computer Forensics
4. General and Application Controls for Information Systems
5. Management Challenges of Security and Control
6. Software Vulnerability and Reliability

Video Cases

Case 1: Stuxnet and Cyberwarfare

Case 2: Cyberespionage: The Chinese Threat

Case 3: IBM Zone Trusted Information Channel (ZTIC)

Instructional Video 1: Sony PlayStation Hacked; Data Stolen from 77 Million Users

Instructional Video 2: Zappos Working to Correct Online Security Breach

Instructional Video 3: Meet the Hackers: Anonymous Statement on Hacking SONY

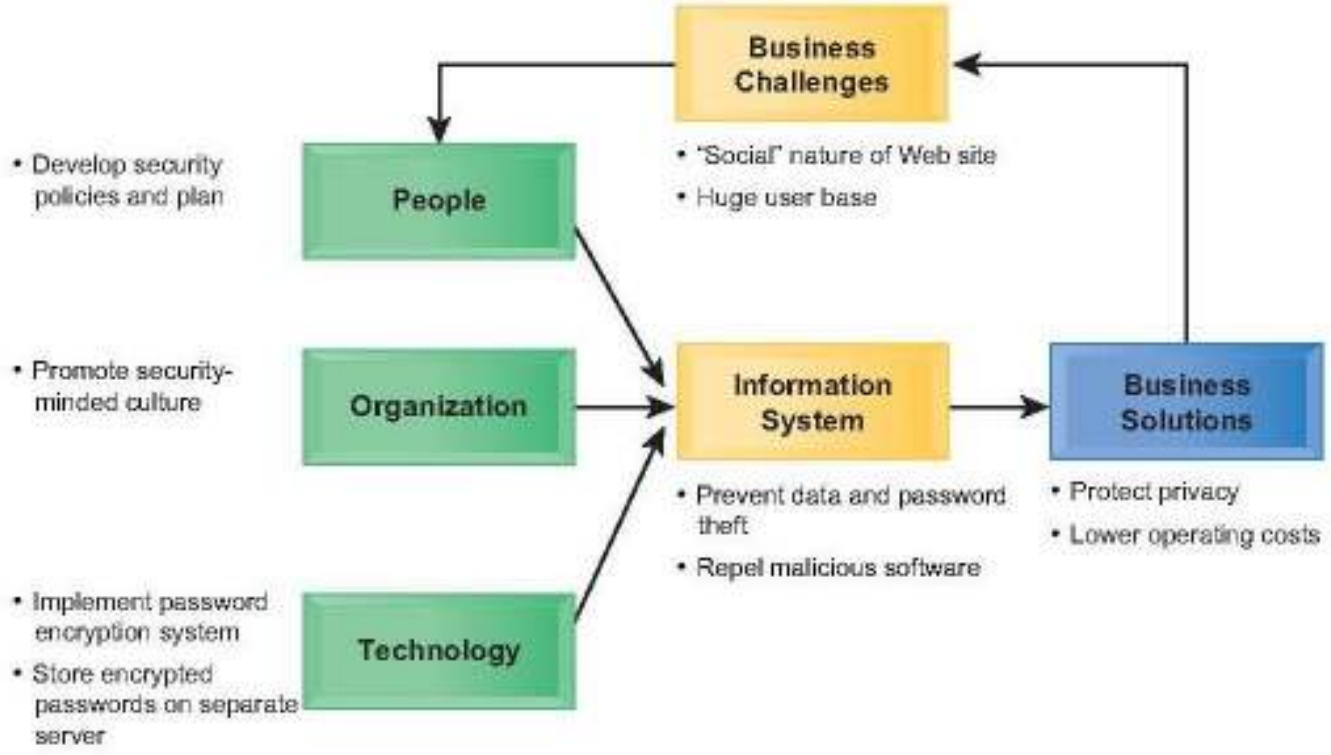
MiniDuke Exposes EU Cybersecurity Gaps

- **Problem**
  - Security breach infects government computers in over 20 European countries
  - Leak of geopolitical intelligence
  - Fragmented approach to cybersecurity in the EU leads to disjointed and disparate policies, and unequal levels of protection.

MiniDuke Exposes EU Cybersecurity Gaps

- **ENISA** urged implementation of a common cybersecurity strategy but EC3 has not been able to stipulate a clear definition for cyber security.
- **Illustrates:** Lack of a centralized and cohesive approach to cybersecurity
- **Demonstrates:** Need for updating security policies continuously and convincing member nations to participate in a consistent, common cybersecurity strategy.

MiniDuke Exposes EU Cybersecurity Gaps



Why Are Information Systems Vulnerable?

- **An unprotected computer connected to Internet may be disabled within seconds**
- **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

Why Systems Are Vulnerable

- **Hardware problems**
  - Breakdowns, configuration errors, damage from improper use or crime
- **Software problems**
  - Programming errors, installation errors, unauthorized changes
- **Disasters**
  - Power failures, flood, fires, and so on
- **Use of networks, computers outside of firm's control**
  - Domestic or offshore outsourcing vendors
  - Mobile devices

Why Are Information Systems Vulnerable?

Contemporary Security Challenges and Vulnerabilities

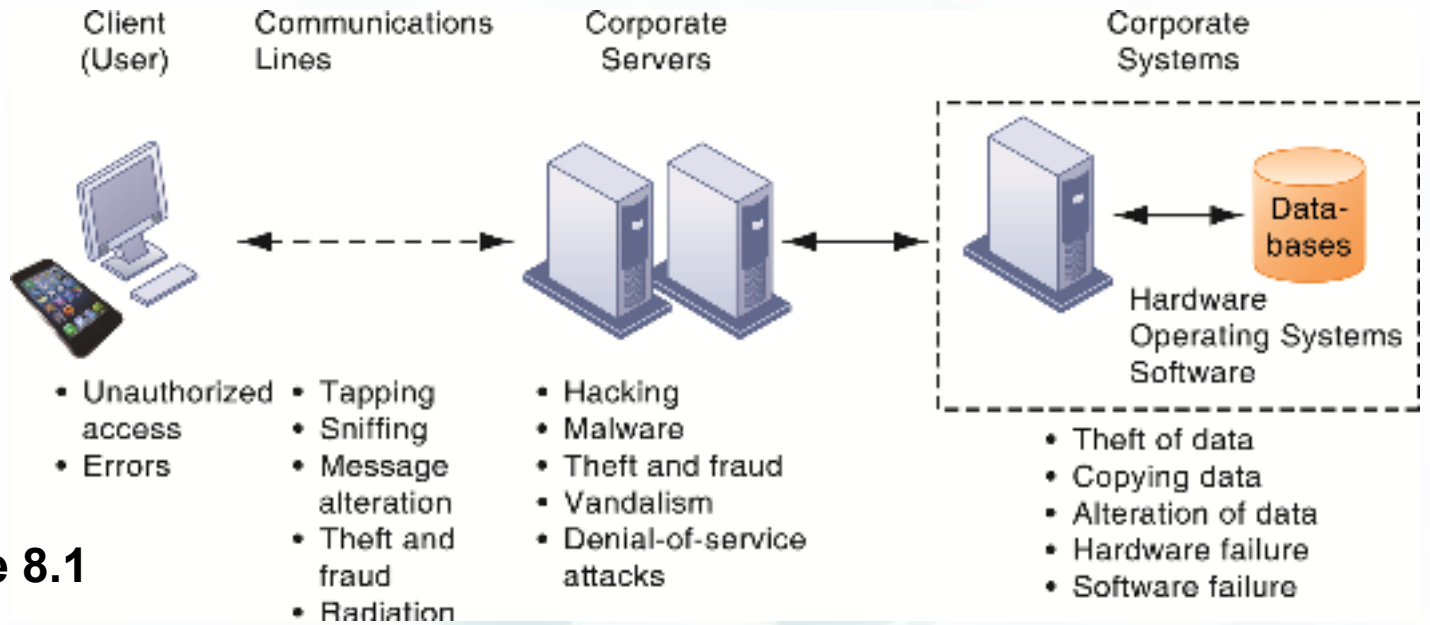


Figure 8.1

The architecture of a Web-based application typically includes a Web client, a server, and corporate information systems linked to databases. Each of these components presents security challenges and vulnerabilities. Floods, fires, power failures, and other electrical problems can cause disruptions at any point in the network.

Why Are Information Systems Vulnerable?

- **Internet vulnerabilities**
  - Network open to anyone
  - Size of Internet means abuses can have wide impact
  - Use of fixed Internet addresses with permanent connections to Internet eases identification by hackers
  - E-mail attachments, file downloading and sharing
  - E-mail used for transmitting trade secrets
  - IM messages lack security, can be easily intercepted

Why Are Information Systems Vulnerable?

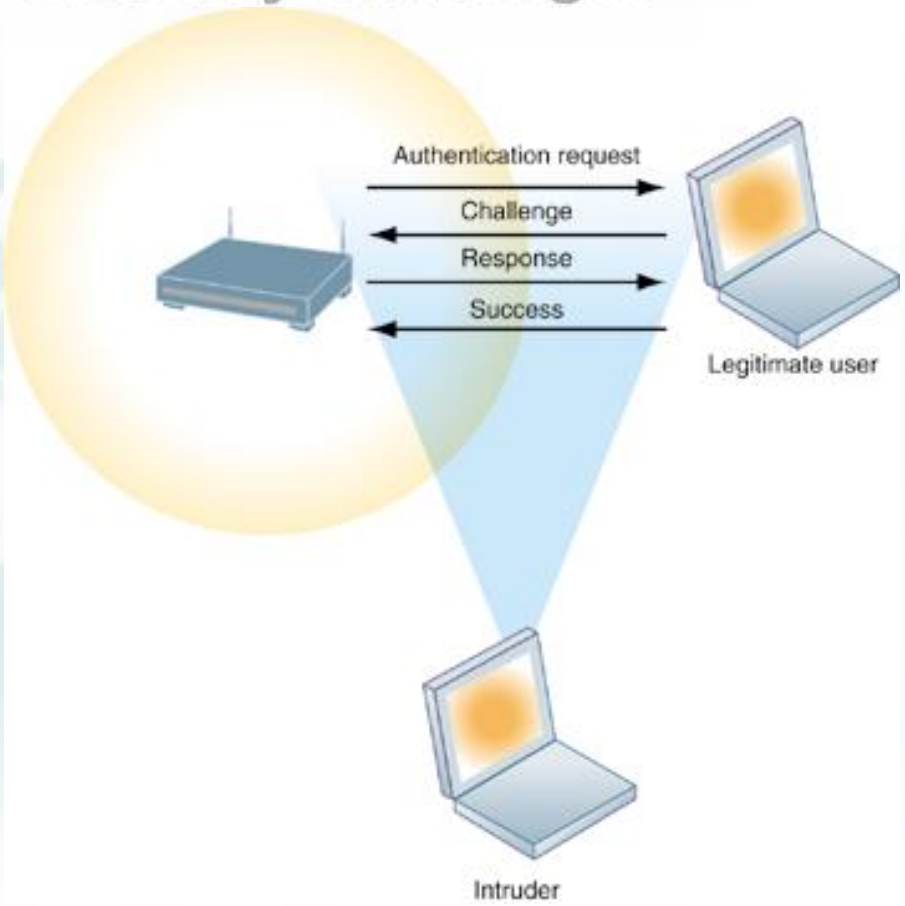
- **Wireless security challenges**
  - **Radio frequency bands easy to scan**
  - **SSIDs (service set identifiers)**
    - Identify access points.
    - Broadcast multiple times.
  - **War driving**
    - Eavesdroppers drive by buildings and try to intercept network traffic
    - With access to SSID, has access to network's resources
  - **Rogue access points**

Why Are Information Systems Vulnerable?

Wi-Fi Security Challenges

Figure 8.2

Many Wi-Fi networks can be penetrated easily by intruders using sniffer programs to obtain an address to access the resources of a network without authorization.



Malicious Software: Viruses, Worms, Trojan Horses, and Spyware

- **Malware**
  - **Viruses**
    - Rogue software program that attaches itself to other software programs or data files in order to be executed
  - **Worms**
    - Independent computer programs that copy themselves from one computer to other computers over a network
  - **Trojan horses**
    - Software program that appears to be benign but then does something other than expected.

Malicious Software: Viruses, Worms, Trojan Horses, and Spyware

- **SQL injection attacks**
- **Spyware**
  - Small programs install themselves surreptitiously on computers to monitor user Web surfing activity and serve up advertising
- **Key loggers**
  - Record every keystroke on computer to steal serial numbers, passwords, launch Internet attacks

Hackers and Computer Crime

- **Hackers versus crackers**
- **Activities include:**
  - **System intrusion**
  - **Theft of goods and services**
  - **System damage**
  - **Cybervandalism —** Intentional disruption, defacement, destruction of Web site or corporate information system

Hackers and Computer Crime

- **Spoofing**
  - Misrepresenting oneself by using fake e-mail addresses or masquerading as someone else
  - Redirecting Web link to address different from intended one, with site masquerading as intended destination
- **Sniffer**
  - Eavesdropping program that monitors information traveling over network
  - Enables hackers to steal proprietary information such as e-mail, company files, and so on

Hackers and Computer Crime

- **Denial-of-service attacks (DoS)**
  - Flooding server with thousands of false requests to crash the network.
- **Distributed denial-of-service attacks (DDoS)**
  - Use of numerous computers to launch a DoS
  - **Botnets**
    - Networks of "zombie" PCs infiltrated by bot malware

Hackers and Computer Crime

- **Computer crime**
  - Any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution
  - **Computer may be target of crime:**
    - Breaching confidentiality of protected computerized data
    - Accessing a computer system without authority
  - **Computer may be instrument of crime:**
    - Theft of trade secrets
    - Using e-mail for threats or harassment

Hackers and Computer Crime

- **Identity theft**
  - Theft of personal information (social security id, driver's license, or credit card numbers) to impersonate someone else
- **Phishing**
  - Setting up fake Web sites or sending e-mail messages that look like legitimate businesses to ask users for confidential personal data
- **Evil twins**
  - Wireless networks that pretend to offer trustworthy Wi-Fi connections to the Internet

Hackers and Computer Crime

- **Pharming**
  - Redirects users to a bogus Web page, even when individual types correct Web page address into his or her browser
- **Click fraud**
  - Fraudulent clicks on online ads
- **Global threats**
  - **Cyberterrorism**
  - **Cyberwarfare**

Internal Threats: Employees

- **Security threats often originate inside an organization.**
  - **Inside knowledge**
  - **Sloppy security procedures**
    - User lack of knowledge
  - **Social engineering:**
    - Tricking employees into revealing their passwords by pretending to be legitimate members of the company in need of information

Software Vulnerability

- **Commercial software contains flaws that create security vulnerabilities.**
  - Hidden bugs (program code defects)
    - Zero defects cannot be achieved because complete testing is not possible with large programs
  - Flaws can open networks to intruders
- **Zero-day Vulnerabilities**
  - Can't protect against malware you don't know about
  - Surprise: there's new malware everyday
  - Anti-malware and virus programs always behind

Why Are Information Systems Vulnerable?

- **Patches:** Small pieces of software to repair flaws released by vendors
  - However, amount of software in use, and shear number of malware programs, can mean exploits are created faster than patches can be released
    - Large number of software applications
    - Disparate operating systems
    - Poor management of patches

What is the Business Value of Security and Control?

- Failed computer systems can lead to significant or total loss of business function.
- Firms now more vulnerable than ever.
- A security breach may cut into firm's market value almost immediately.
- Inadequate security and controls also bring forth issues of liability.

Legal and Regulatory Requirements for Electronic Records Management

- Firms face new legal obligations for the retention and storage of electronic records as well as for privacy protection
  - **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 Forensics

- **Evidence for white collar crimes often found in digital form**
  - Data stored on computer devices, e-mail, instant messages, e-commerce transactions
- **Proper control of data can save time, 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
  - Includes recovery of ambient and hidden data

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

- **Information systems controls**
  - **General controls**
    - Govern design, security, and use of computer programs and security of data files in general throughout organization's information technology infrastructure.
    - Apply to all computerized applications.
    - Combination of hardware, software, and manual procedures to create overall control environment.

Components of an organizational framework for security and control

- **Types of general controls**
  - Software controls
  - Hardware controls
  - Computer operations controls
  - Data security controls
  - Implementation controls
  - Administrative controls

Components of an organizational framework for security and control

- **Application controls**
  - Specific controls unique to each computerized application, such as payroll or order processing.
  - Include both automated and manual procedures.
  - Ensure that only authorized data are completely and accurately processed by that application.
  - Include:
    - **Input controls**
    - **Processing controls**
    - **Output controls**

Components of an organizational framework for security and control

- **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**

EXPOSURE	PROBABILITY	LOSS RANGE	EXPECTED ANNUAL LOSS
Power failure	30%	$5K - $200K	$30,750
Embezzlement	5%	$1K - $50K	$1,275
User error	98%	$200 - $40K	$19,698

Interactive Session: Organizations
Stuxnet and the Changing Face of Cyberwarfare

Read the Interactive Session and answer the following questions:

- Is cyberwarfare a serious problem? Why or why not?
- Assess the management, organization, and technology factors that have created this problem.
- What makes Stuxnet different from other cyberwarfare attacks? How serious a threat is this technology?
- What solutions have been proposed for this problem? Do you think they will be effective? Why or why not?

Components of an organizational framework for security and control

- **Security policy**
  - **Ranks information risks**
  - **Identifies acceptable security goals**
  - **Identifies mechanisms for achieving these goals**
  - **Drives other policies**
    - Acceptable use policy (AUP)
    - Authorization policies
  - **Provisions for identity management**

Components of an organizational framework for security and control

- **Identity management**
  - Business process and technologies for identifying valid users of system
  - Creates different levels or roles of system user and access
  - Allows each user access only to those portions of system that user role

Components of an organizational framework for security and control

Security Profiles for a Personnel System

Figure 8.3

These two examples represent two security profiles or data security patterns that might be found in a personnel system. Depending on the security profile, a user would have certain restrictions on access to various systems, locations, or data in an organization.

SECURITY PROFILE 1

User: Personnel Dept. Clerk

Location: Division 1

Employee Identification Codes with This Profile: 00753, 27834, 37665, 44116

Data Field Restrictions	Type of Access
All employee data for Division 1 only	Read and Update
• Medical history data	None
• Salary	None
• Pensionable earnings	None

SECURITY PROFILE 2

User: Divisional Personnel Manager

Location: Division 1

Employee Identification Codes with This Profile: 27321

Data Field Restrictions	Type of Access
All employee data for Division 1 only	Read Only

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

- **MIS audit**
  - Examines firm's overall security environment as well as controls governing individual information systems
  - Reviews technologies, procedures, documentation, training, and personnel
  - May even simulate disaster to test response of technology, IS staff, other employees
  - Lists and ranks all control weaknesses and estimates probability of their occurrence.
  - Assesses financial and organizational impact of each threat

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

Sample Auditor's List of Control Weaknesses

Figure 8.4

This chart is a sample page from a list of control weaknesses that an auditor might find in a loan system in a local commercial bank. This form helps auditors record and evaluate control weaknesses and shows the results of discussing those weaknesses with management, as well as any corrective actions taken by management.

Function: Loans Location: Peoria, IL	Prepared by: J. Ericson Date: June 16, 2014		Received by: T. Benson Review date: June 28, 2014	
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	5/10/14	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	5/10/14	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		

Most important tools and technologies for safeguarding information resources

Identity Management and Authentication

- Authentication
  - Password systems
  - Tokens
  - Smart cards
  - Biometric authentication
    - Fingerprints, irises, voices

Most important tools and technologies for safeguarding information resources

Firewalls, Intrusion Detection Systems, and Antivirus Software

- Firewall:
  - Combination of hardware and software that prevents unauthorized access to network
  - Technologies include:
    - Packet filtering
    - Stateful inspection
    - Network address translation (NAT)
    - Application proxy filtering

Most important tools and technologies for safeguarding information resources

A Corporate Firewall

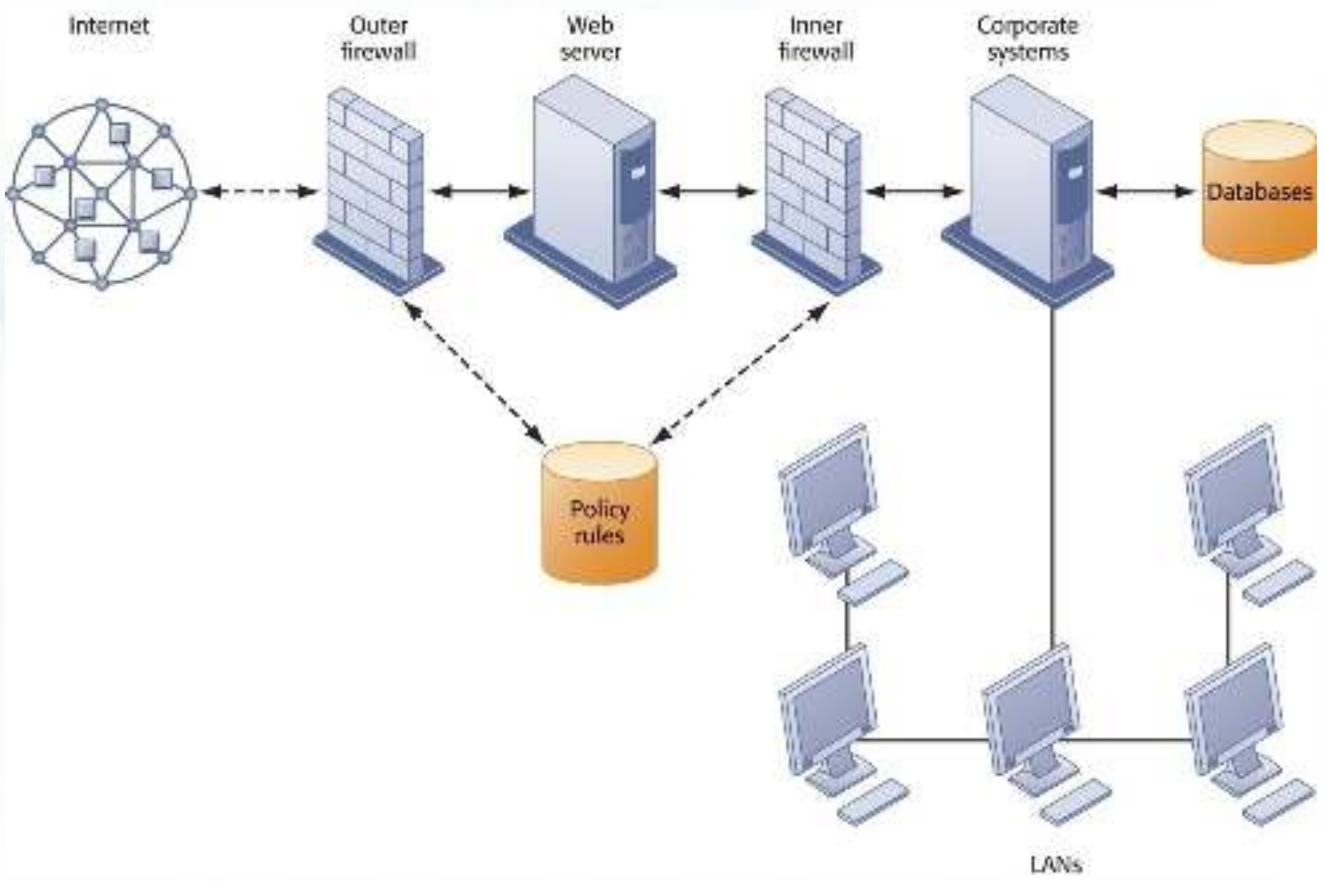


Figure 8.5

The firewall is placed between the firm's private network and the public Internet or another distrusted network to protect against unauthorized traffic.

Most important tools and technologies for safeguarding information resources

- **Intrusion detection systems:**
  - Monitor hot spots on corporate networks to detect and deter intruders.
  - Examine events as they are happening to discover attacks in progress.
- **Antivirus and antispyware software:**
  - Check computers for presence of malware and can often eliminate it as well.
  - Require continual updating.
- **Unified Threat Management (UTM) systems**

Most important tools and technologies for safeguarding information resources

Securing Wireless Networks

- **WEP security can be improved:**
  - Activating it
  - Assigning unique name to network's SSID
  - Using it with VPN technology
- **Wi-Fi Alliance finalized WPA2 specification, replacing WEP with stronger standards**
  - Continually changing keys
  - Encrypted authentication system with central server

Encryption and Public Key Infrastructure

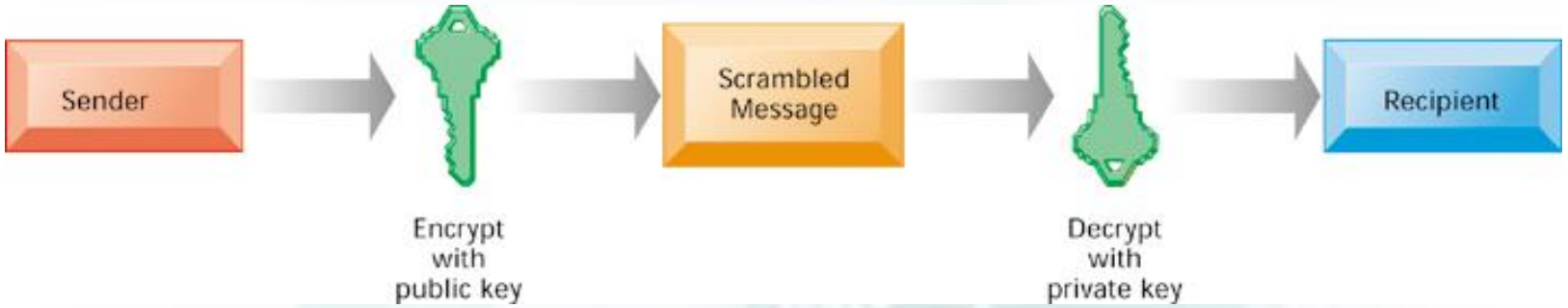
- Encryption:
  - Transforming text or data into cipher text that cannot be read by unintended recipients
  - Two methods for encryption on networks
    - Secure Sockets Layer (SSL) and successor Transport Layer Security (TLS)
    - Secure Hypertext Transfer Protocol (S-HTTP)

Encryption and Public Key Infrastructure

- **Two methods of encryption**
  - **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

Most important tools and technologies for safeguarding information resources

Public Key Encryption



A public key encryption system can be viewed as a series of public and private keys that lock data when they are transmitted and unlock the data when they are received. The sender locates the recipient's public key in a directory and uses it to encrypt a message. The message is sent in encrypted form over the Internet or a private network. When the encrypted message arrives, the recipient uses his or her private key to decrypt the data and read the message.

Figure 8.6

Most important tools and technologies for safeguarding information resources

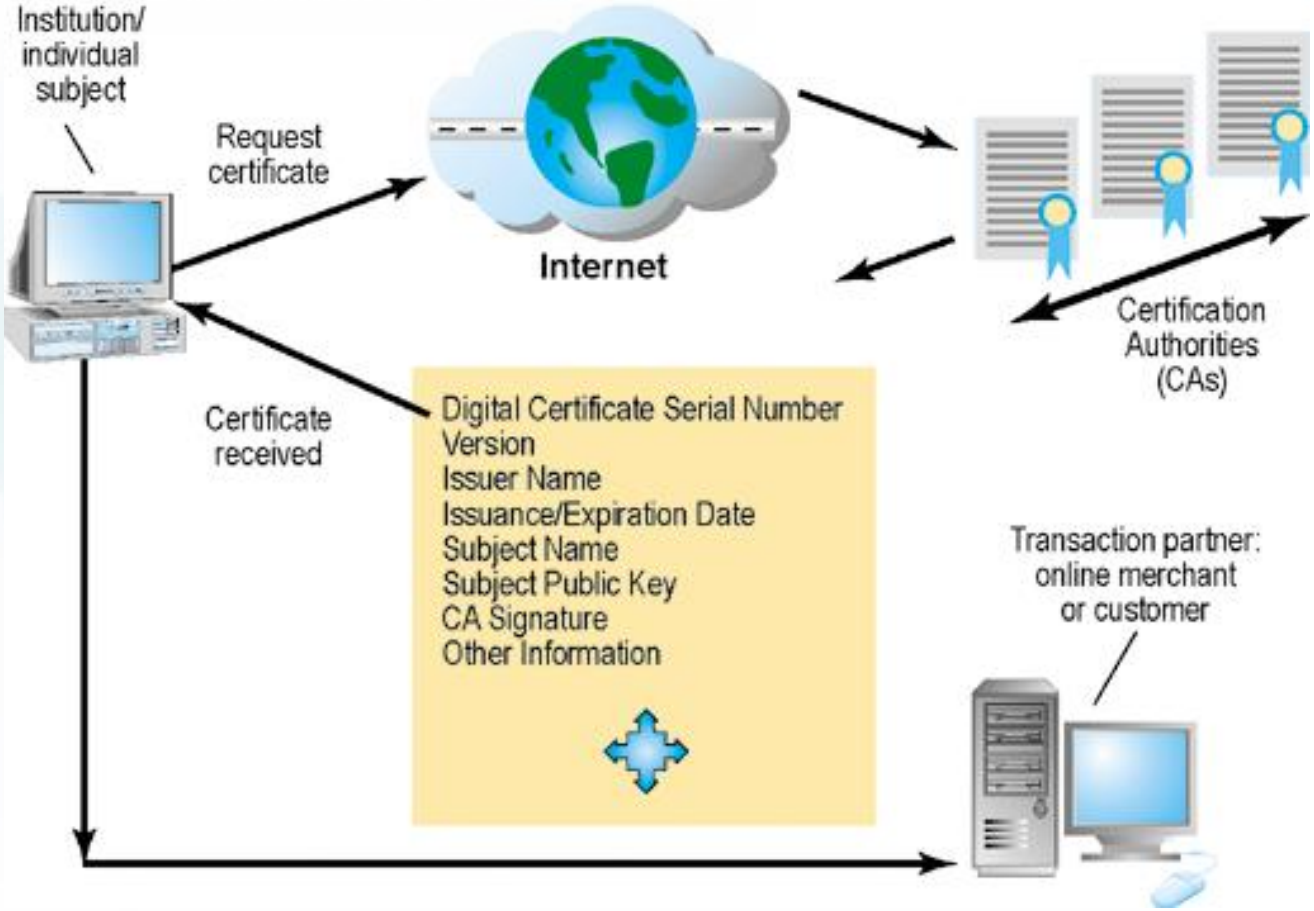
- **Digital certificate:**
  - Data file used to establish the identity of users and electronic assets for protection of online transactions
  - Uses certification authority (CA) to validate a user's identity
  - CA verifies user's identity, stores information in CA server, which generates encrypted 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

Most important tools and technologies for safeguarding information resources

Digital Certificates

Figure 8.7

Digital certificates help establish the identity of people or electronic assets. They protect online transactions by providing secure, encrypted, online communication.



Ensuring System Availability

- **Online transaction processing requires 100 percent availability, no downtime.**
- **Fault-tolerant computer systems**
  - For continuous availability, e.g., stock markets
  - Contain redundant hardware, software, and power supply components that create an environment that provides continuous, uninterrupted service
- **High-availability computing**
  - Helps recover quickly from crash
  - Minimizes, does not eliminate, downtime

Most important tools and technologies for safeguarding information resources

Ensuring System Availability

- **Recovery-oriented computing**
  - Designing systems that recover quickly with capabilities to help operators pinpoint and correct faults in multicomponent systems
- **Controlling network traffic**
  - Deep packet inspection (DPI) (video and music blocking)
- **Security outsourcing**
  - Managed security service providers (MSSPs)

Security Issues for Cloud Computing

- **Cloud computing**
  - Highly distributed computing, difficult to track unauthorized activities
  - Cloud users should ask for proof of security and privacy procedures, including encryption
  - Service level agreements (SLAs)

Security Issues for the Mobile Digital Platform

- **Mobile platforms**
  - Mobile device management tools for authorization and inventory
  - Data loss prevention technology
  - Mobile security policies: platform, software, procedures, security products
  - Encryption
  - BYOD
  - Mobile protective software products

The Flash Crash: A New Culprit

Interactive Session: Technology
MWEB Business Hacked

Read the Interactive Session and answer the following questions:

- What security and control problems are described in this case?
- What people, organization, and technology factors contribute to these problems?
- How secure is cloud computing? Explain your answer.
- If you were in charge of your company's information systems department, what issues would you want to clarify with prospective vendors?
- Would you entrust your corporate systems to a cloud computing provider? Why or why not?

Ensuring Software Quality

- **Software Metrics:** objective assessments of system in form of quantified measurements, e.g.:
  - 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