# Chapter 8

# Securing Information Systems

## LEARNING OBJECTIVES

- Explain why information systems are vulnerable to destruction, error, and abuse.
- Assess the business value of security and control.
- Identify the components of an organizational framework for security and control.
- Evaluate the most important tools and technologies for safeguarding information resources.

## Boston Celtics Score Big Points Against Spyware

- **Problem:** Spyware infecting laptops during team travel affecting accessibility and performance of proprietary system
- **Solutions: Deploy security software** to reduce spyware.
- **Mi5 Network's Webgate security appliance** tool sits between corporate firewall and network to prevent spyware entering network or infected computers connecting to network
- Demonstrates IT's role in combating malicious software
- Illustrates digital technology's role in achieving security on the Web

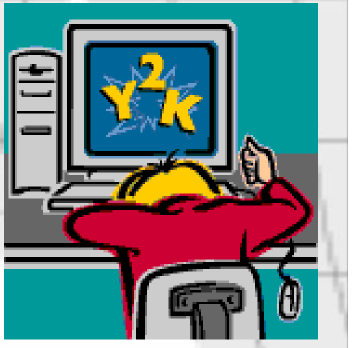
**Organizations need to make security and control a top priority to prevent destruction, error and abuse**

- **Security:**
  - Policies, procedures and technical measures used to prevent unauthorized access, alteration, theft, or physical damage to information systems

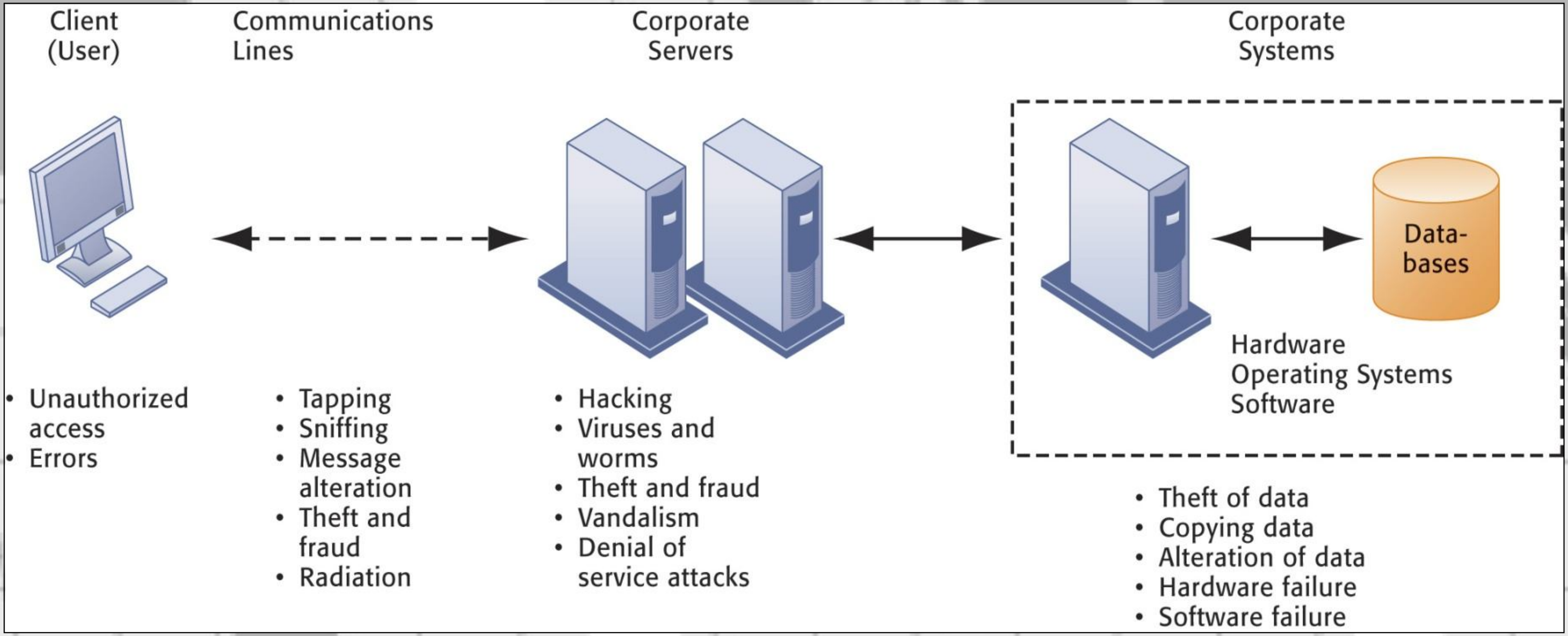
- **Controls:**
  - Methods, policies, and organizational procedures that ensure safety of organization’s assets; accuracy and reliability of its accounting records; and operational adherence to management standards

## System Vulnerability and Abuse

- **Why systems are vulnerable to destruction, error and abuse**
  - **Hardware problems**
    - Breakdowns, configuration errors, damage from improper use or crime
  - **Software problems**
    - Programming errors, installation errors, unauthorized changes)
  - **Disasters**
    - Power failures, flood, fires, earthquakes, etc.
  - **Use of networks and computers outside of firm's control**
    - E.g., with domestic or offshore outsourcing vendors



# Contemporary Security Challenges and Vulnerabilities



Client (User)

- Unauthorized access
- Errors

Communications Lines

- Tapping
- Sniffing
- Message alteration
- Theft and fraud
- Radiation

Corporate Servers

- Hacking
- Viruses and worms
- Theft and fraud
- Vandalism
- Denial of service attacks

Corporate Systems

- Theft of data
- Copying data
- Alteration of data
- Hardware failure
- Software failure

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.

Figure 8-1

## System Vulnerability and Abuse

- 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
  - E-mail used for transmitting trade secrets
  - IM messages lack security, can be easily intercepted

## System Vulnerability and Abuse

- **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
    - When hacker gains access to SSID, has access to network's resources
  - **WEP (Wired Equivalent Privacy)**
    - Security standard for 802.11
    - Basic specification uses shared password for both users and access point
    - Users often fail to use security features

System Vulnerability and Abuse

# Wi-Fi Security Challenges

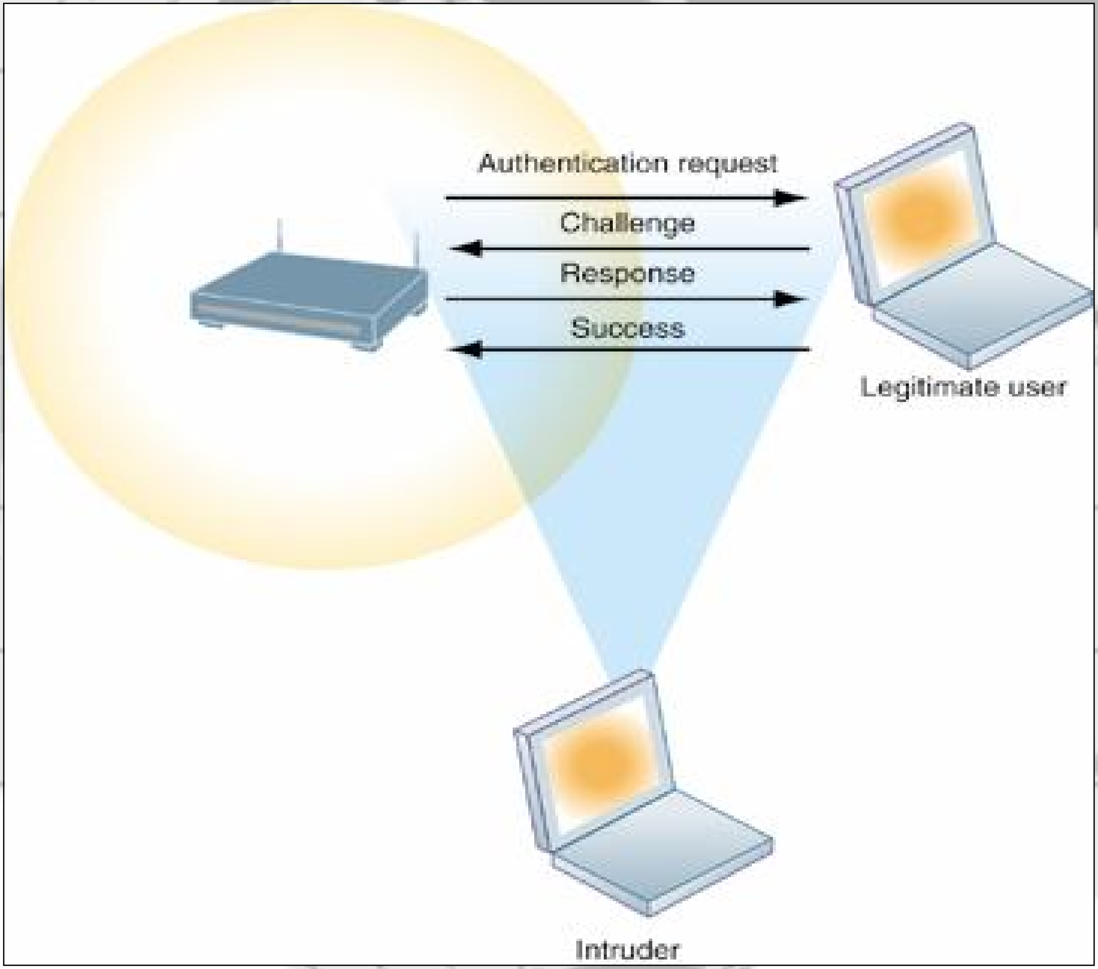


**Figure 8-2**

**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.**

# The Worst Data Theft Ever?

- **Read the Interactive Session: Organizations and then discuss the following questions:**
  - **List and describe the security control weaknesses at TJX Companies**
  - **What management, organization, and technology factors contributed to these weaknesses?**
  - **What was the business impact of TJX's data loss on TJX, consumers, and banks?**
  - **How effectively did TJX deal with these problems?**
  - **Who should be held liable for the losses caused by the use of fraudulent credit cards in this case? The banks issuing the cards or the consumers? Justify your answer.**
  - **What solutions would you suggest to prevent the problems?**

## System Vulnerability and Abuse

- **Malicious software (malware)**
  - **Viruses:** Rogue software program that attaches itself to other software programs or data files in order to be executed. Typically spread when sending e-mail attachment or copying file. Highly destructive e.g. destroying programs /data, clogging computer memory, programs run improperly.
  - **Worms:** Independent computer programs that copy themselves from one computer to other computers over a network. Destroy data/programs, disrupt/ halt computer network operation.
  - **Trojan horses:** Software program that appears to be benign but then does something other than expected
  - **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

## System Vulnerability and Abuse

- Hackers and computer crime
  - Hackers vs. crackers
  - Activities include
    - System intrusion
    - Theft of goods and information
    - System damage
    - Cybervandalism
      - Intentional disruption, defacement, destruction of Web site or corporate information system

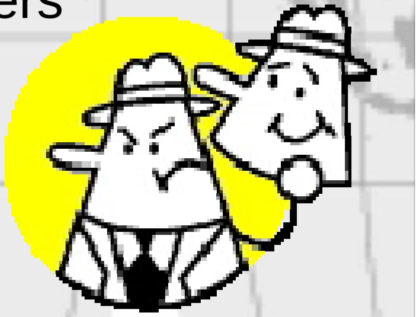
## System Vulnerability and Abuse

- **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. Help to identify weak spots on network. Enable hackers to steal information on the network e.g. email, files and reports.
- **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

- **Computer crime**
  - Defined 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, e.g.:**
    - Breaching confidentiality of protected computerized data
    - Accessing a computer system without authority
  - **Computer may be instrument of crime, e.g.:**
    - Theft of trade secrets
    - Using e-mail for threats or harassment

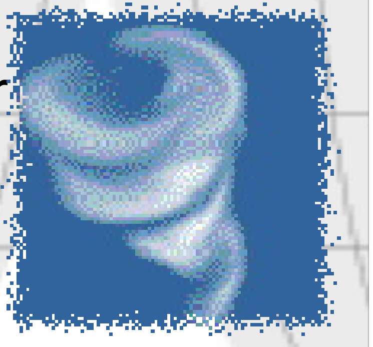
## System Vulnerability and Abuse

- **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
- **Pharming:** Redirects users to a bogus Web page, even when individual types correct Web page address into his or her browser



## System Vulnerability and Abuse

- **Click fraud**
  - Individual or computer program clicks online ad without any intention of learning more or making a purchase. A serious problem at sites that feature pay-per-click on-line advertising.
- **Global threats - Cyberterrorism and cyberwarfare**
  - Concern that Internet vulnerabilities and other networks make digital networks easy targets for digital attacks by terrorists, foreign intelligence services, or other groups



## System Vulnerability and Abuse

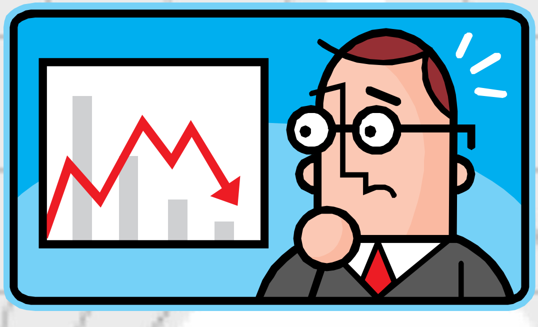
- Internal threats – Employees
  - Security threats often originate inside an organization
    - Inside knowledge
    - Sloppy security procedures
      - User lack of knowledge
    - Social engineering:
      - Tricking employees into revealing their passwords by pretending to be legitimate members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

## System Vulnerability and Abuse

- **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
  - **Patches**
    - Vendors release small pieces of software to repair flaws
    - However, amount of software in use can mean exploits created faster than patches be released and implemented

## Business Value of Security and Control

- Lack of security, control can lead to:
  - Loss of revenue
    - Failed computer systems can lead to significant or total loss of business function
  - Lowered market value:
    - Information assets can have tremendous value
    - A security breach may cut into firm’s market value almost immediately
  - Legal liability
  - Lowered employee productivity
  - Higher operational costs



## Business Value of Security and Control

- **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

## Business Value of Security and Control

- **Electronic evidence**
  - **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

## Establishing a Framework for Security and Control

- **Information systems controls**
  - **General controls**
    - Govern design, security, and use of computer programs and data throughout organization’s IT infrastructure
    - Combination of hardware, software, and manual procedures to create overall control environment
    - Types of general controls
      - **Software controls**
      - **Hardware controls**
      - **Computer operations controls**
      - **Data security controls**
      - **Implementation controls**
      - **Administrative controls**

## Establishing a 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
  - Types of application controls:
    - **Input controls**
    - **Processing controls**
    - **Output controls**

## Establishing a Framework for Security and Control

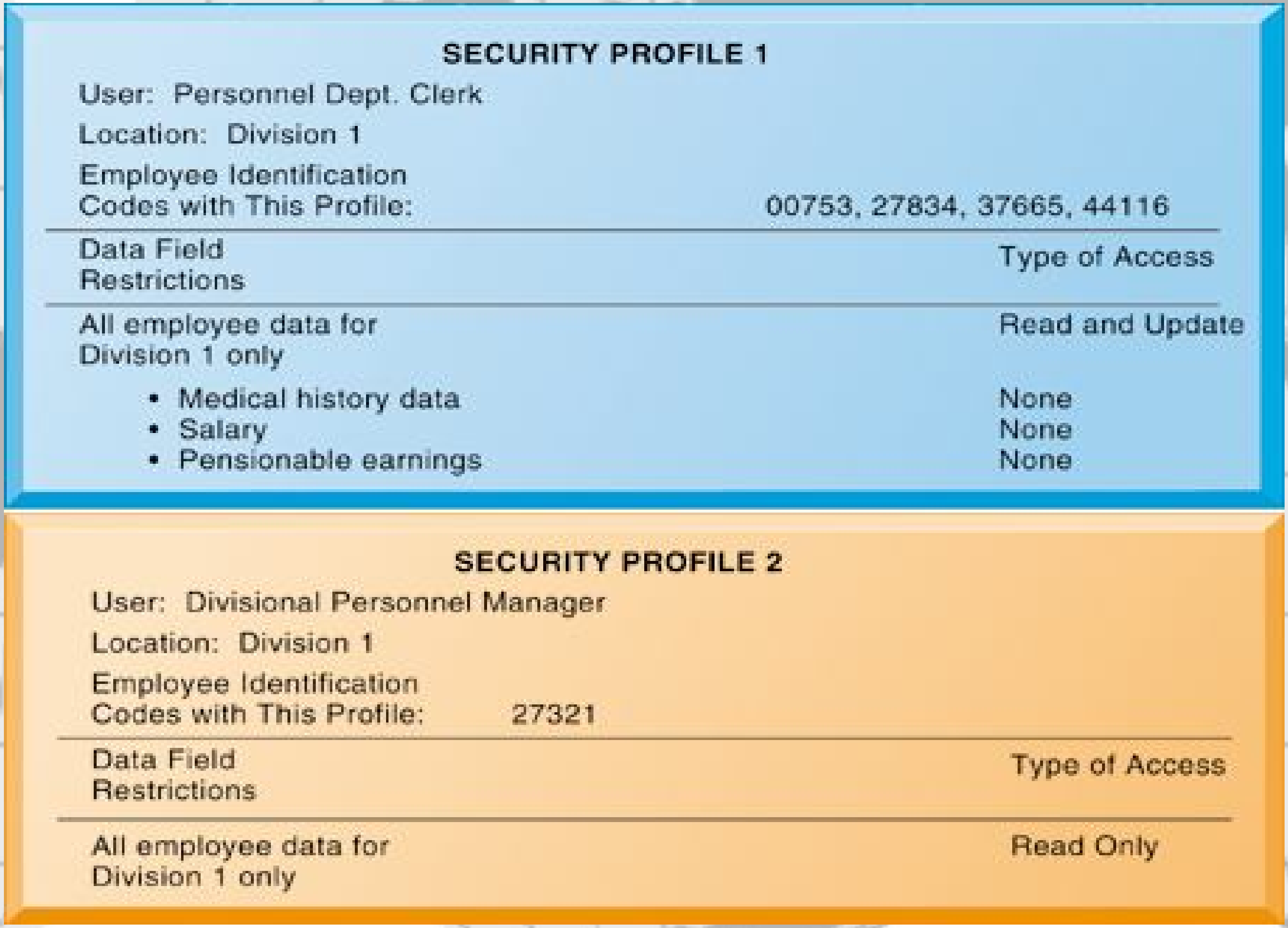
- **Risk assessment**
  - Determines level of risk to firm if specific activity or process is not properly controlled
    - Types of threat
    - Probability of occurrence during year
    - Potential losses, value of threat
    - Expected annual loss

| EXPOSURE | PROBABILITY | LOSS RANGE (AVERAGE) | EXPECTED ANNUAL LOSS |
|---|---|---|---|
| Power failure | 30% | $5K - $200K ($102,500) | $30,750 |
| Embezzlement | 5% | $1K - $50K ($25,500) | $1,275 |
| User error | 98% | $200 - $40K ($20,100) | $19,698 |

## Establishing a Framework for Security and Control

- **Security policy**
  - Ranks information risks, identifies acceptable security goals, and identifies mechanisms for achieving these goals
  - Drives other policies
    - **Acceptable use policy (AUP):** Defines acceptable uses of firm’s information resources and computing equipment
    - **Authorization policies:** Determine differing levels of  user access to information assets
- **Authorization management systems**
  - Allow each user access only to those portions of system that person is permitted to enter, based on information established by set of access rules, profile

# Security Profiles for a Personnel System



**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 |

**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.**

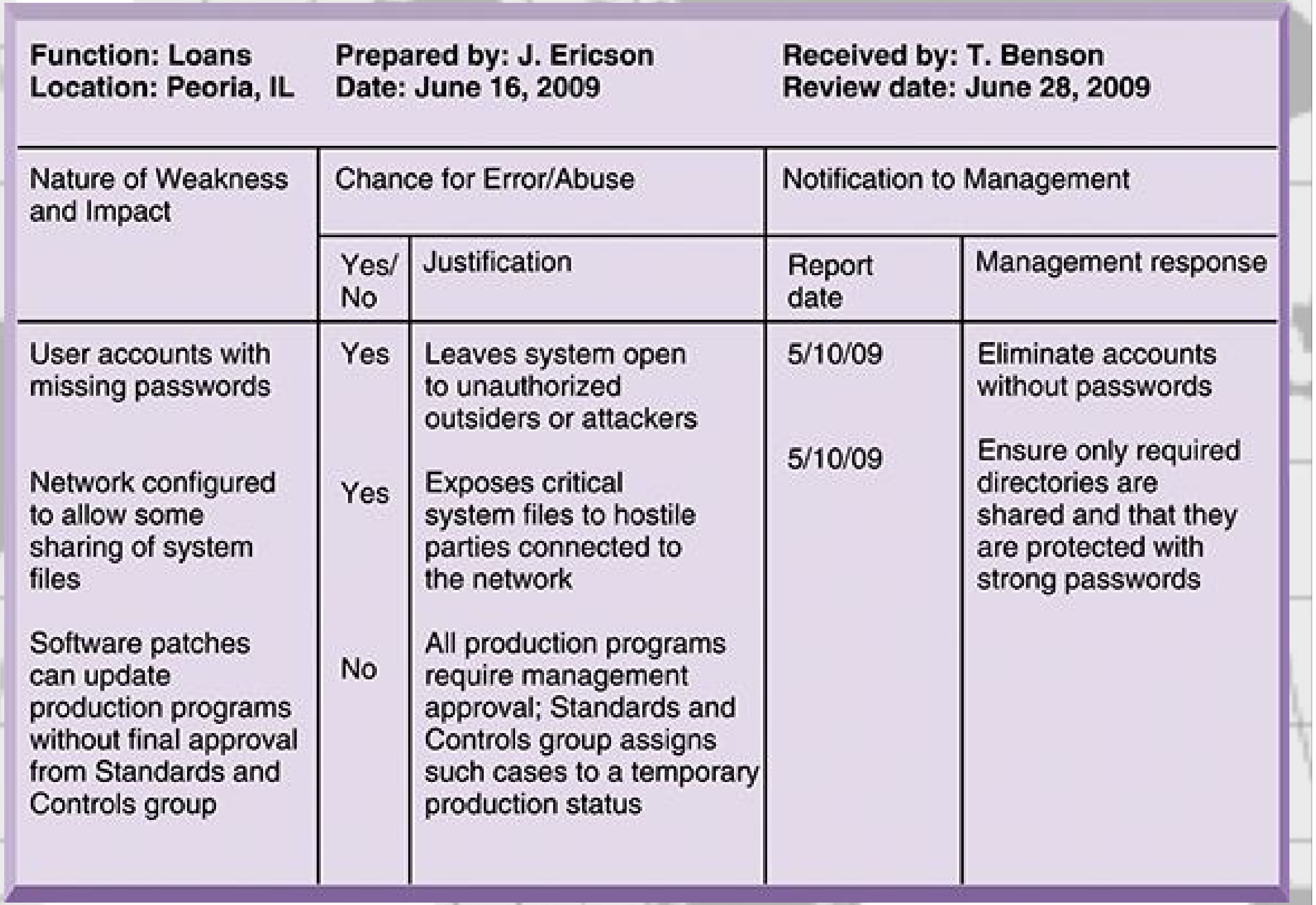
## Establishing a Framework for Security and Control

- **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 and business processes
  - Business impact analysis to determine impact of an outage
  - Management must determine
    - Maximum time systems can be down
    - Which systems must be restored first

## Establishing a Framework for Security and Control

- **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

# Sample Auditor’s List of Control Weaknesses



| | | | | |
|---|---|---|---|---|
| Function: Loans<br>Location: Peoria, IL | Prepared by: J. Ericson<br>Date: June 16, 2009 | | Received by: T. Benson<br>Review date: June 28, 2009 | |
| 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 | 5/10/09 | 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 | 5/10/09 | 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 | | |

**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.**

## Technologies and Tools for Security

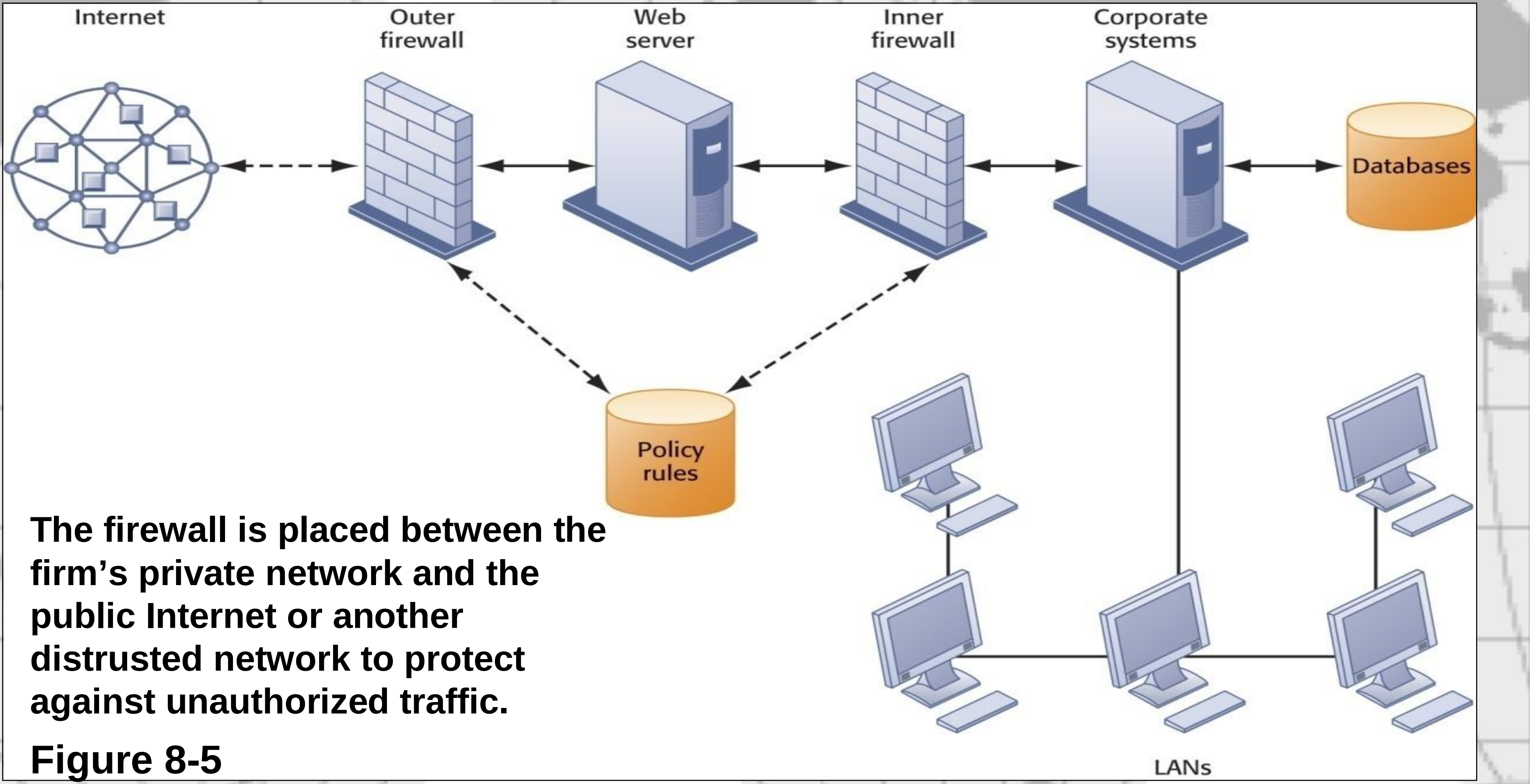
- **Access control: Policies and procedures to prevent improper access to systems by unauthorized insiders and outsiders**
  - **Authorization**
  - **Authentication**
    - **Password systems**
    - **Tokens**
    - **Smart cards**
    - **Biometric authentication**

## Technologies and Tools for Security

- **Firewall:** Hardware and/or software to prevent unauthorized access to private networks
  - Screening technologies
    - Packet filtering
    - Stateful inspection
    - Network address translation (NAT)
    - Application proxy filtering

- **Intrusion detection systems:** Monitor vulnerable points on networks to detect and deter intruders
  - Examines events  as they are happening to discover attacks in progress
  - Scans network to find patterns indicative of attacks

# A Corporate Firewall



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

**Figure 8-5**

## Technologies and Tools for Security

- **Antivirus and antispyware software:**
  - Checks computers for presence of malware and can often eliminate it as well
  - Require continual updating
- Unified threat management (UTM)
  - Comprehensive security management products
  - Tools include
    - Firewalls
    - Intrusion detection
    - VPNs
    - Web content filtering
    - Antispam software

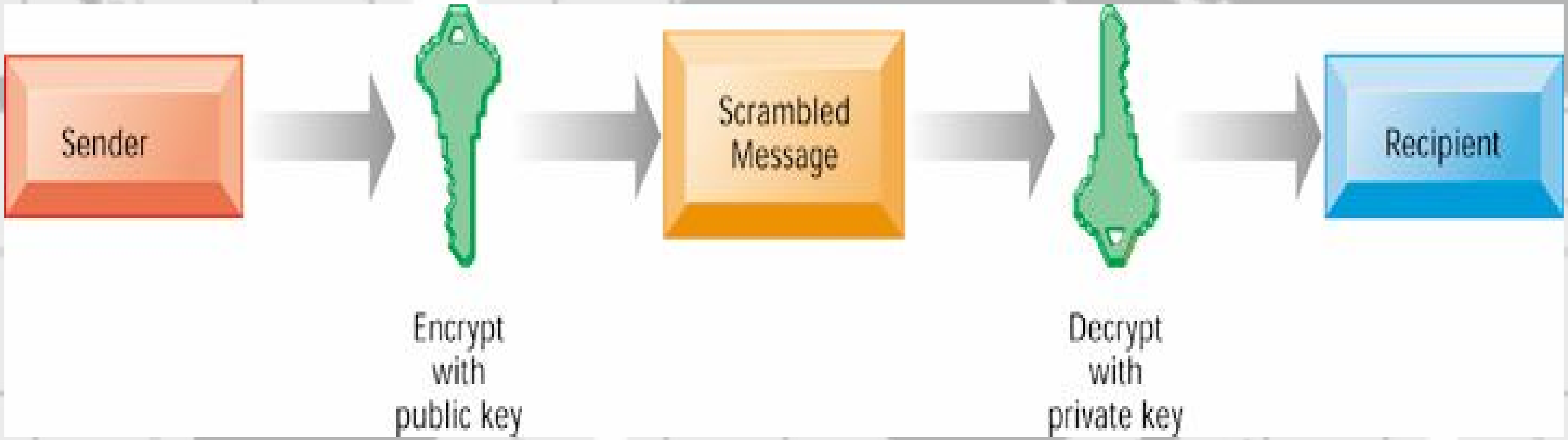
## Technologies and Tools for Security

- **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 WAP2 specification, replacing WEP with stronger standards**
    - Continually changing keys
    - Encrypted authentication system with central server

## Technologies and Tools for Security

- **Encryption:**
  - Transforming text or data into cipher text that cannot be read by unintended recipients
  - **Two methods for encrypting network traffic**
    - Secure Sockets Layer (SSL) and successor Transport Layer Security (TLS)
    - Secure Hypertext Transfer Protocol (S-HTTP)
  - **Two methods of encryption**
    - Symmetric key encryption
    - Public key encryption

# Public Key Encryption



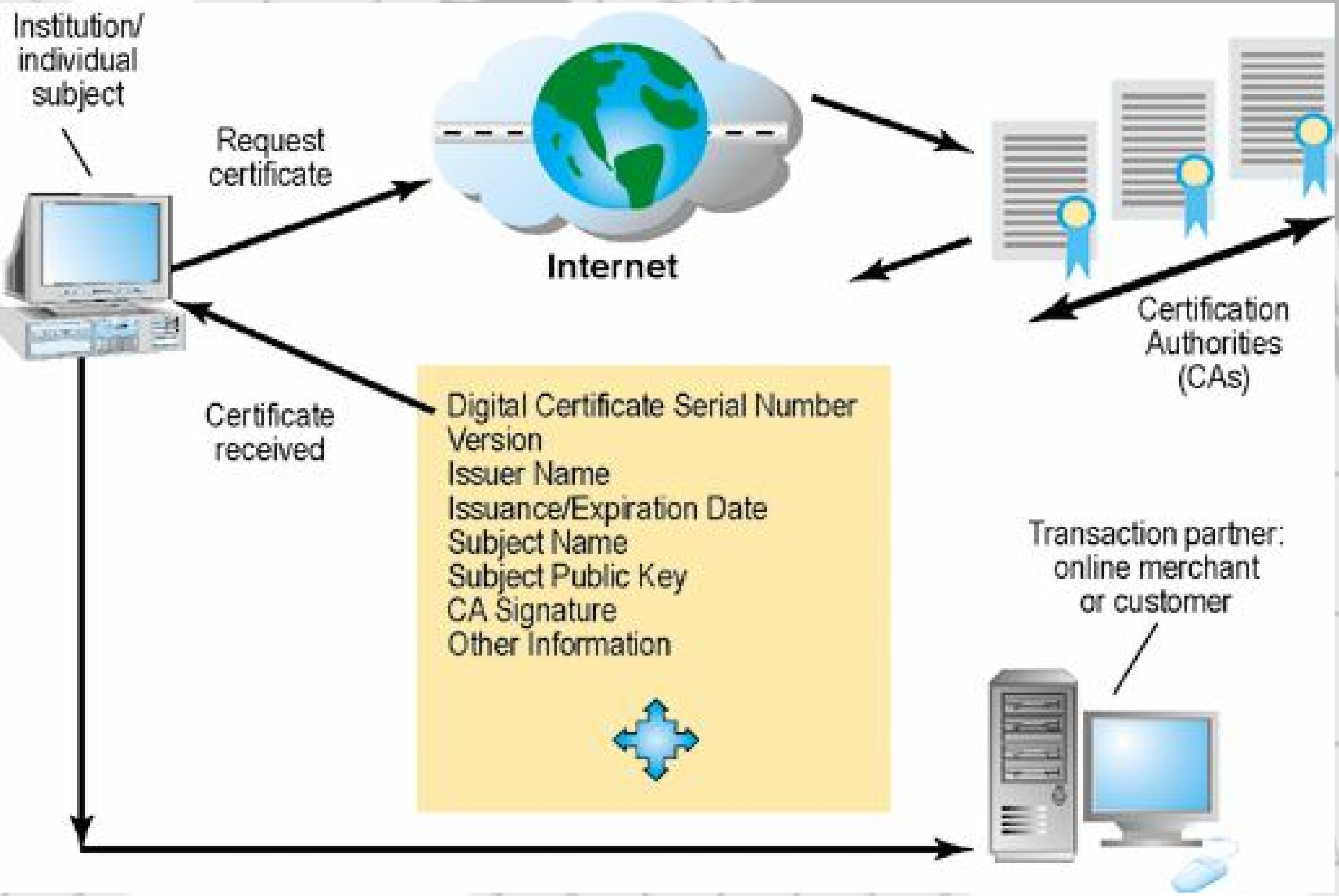
A public key encryption system can be viewed as a series of public and private keys that lock data when they are transmitted and unlock the data when they are received. The sender locates the recipient’s public key in a directory and uses it to encrypt a message. The message is sent in encrypted form 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 7-6

## Technologies and Tools for Security

- **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

# Digital Certificates


Institution/ individual subject
Request certificate
Internet
Certification Authorities (CAs)
Certificate received
Transaction partner: online merchant or customer

Digital Certificate Serial Number
Version
Issuer Name
Issuance/Expiration Date
Subject Name
Subject Public Key
CA Signature
Other Information

**Figure 8-7**

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

## Technologies and Tools for Security

- **Ensuring system availability**
  - **Online transaction processing requires 100% availability, no downtime**
  - **Fault-tolerant computer systems**
    - For continuous availability
    - Contain redundant hardware, software, and power supply components to provide continuous, uninterrupted service
  - **High-availability computing**
    - Helps recover quickly from crash
    - Minimizes, does not eliminate downtime

## Technologies and Tools for Security

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

# Can Salesforce.com On-Demand Remain in Demand?

- Read the Interactive Session: Technology and then discuss the following questions:
  - How did the problems experienced by Salesforce.com impact its business?
  - How did the problems impact its customers?
  - What steps did Salesforce.com take to solve the problems? Were these steps sufficient?
  - List and describe other vulnerabilities discussed in this chapter that might create outages at Salesforce.com and measures to safeguard against them.

## Technologies and Tools for Security

- **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
  - **Testing: Early and regular testing**
    - **Walkthrough:** Review of specification or design document by small group of qualified people
    - **Debugging:** Process by which errors are eliminated

# What is the business value of security and control? Explain how security and control provide value for businesses.

Security refers to the policies, procedures, and technical measures used to prevent unauthorized access, alteration, theft, or physical damage to information systems.

Controls consist of all the methods, policies, and organizational procedures that ensure the safety of the organization’s assets; the accuracy and reliability of its account records; and operational adherence to management standards.

Security and control provide business value by:

•Firms relying on computer systems for their core business functions can lose sales and productivity.

•Information assets, such as confidential employee records, trade secrets, or business plans, lose much of their value if they are revealed to outsiders or if they expose the firm to legal liability.