Chapter 8

Securing Information Systems

nagement Information Systems

apter 8 Securing Information Systems

System Vulnerability and Abuse

Å **Security:**

Å Policies, procedures and technical measures used to prevent unauthorized access, alteration, theft, or physical damage to information systems

Å **Controls:**

Å Methods, policies, and organizational procedures that ensure safety of organizationŝ assets; accuracy and reliability of its accounting records; and operational adherence to management standards

System Vulnerability and Abuse

Å **Why systems are vulnerable**

Å **Hardware problems**

Å Breakdowns, configuration errors, damage from improper use or crime

Å **Software problems**

Å Programming errors, installation errors, unauthorized changes)

Å **Disasters**

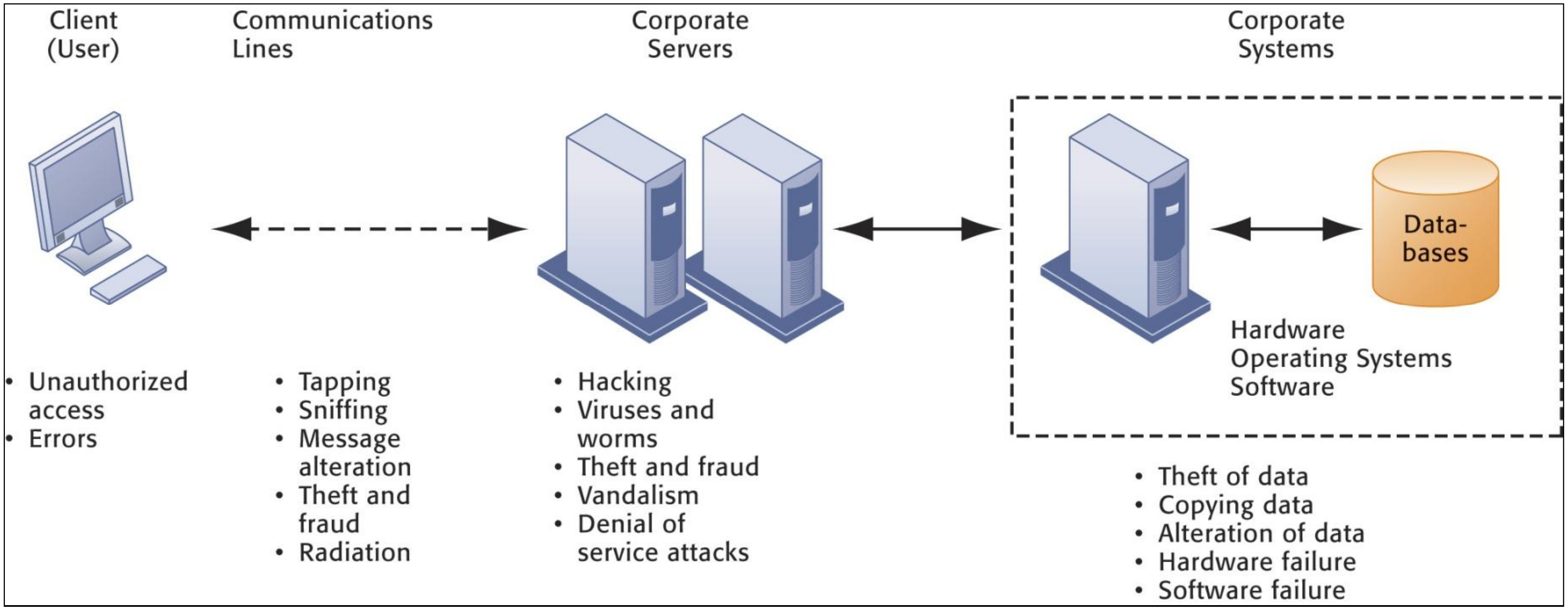
Å Power failures, flood, fires, etc.

Å **Use of networks and computers outside of firm’s control**

Å E.g., with domestic or offshore outsourcing vendors

System Vulnerability and Abuse

Contemporary Security Challenges and Vulnerabilities



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

Å Internet Vulnerability/weaknesses

- Å Network open to anyone.
- Å Size of Internet means abuses (bad usage) can have wide impact.
- Å Use of fixed Internet addresses with permanent connections to Internet eases identification by hackers.
- Å E-mail attachments.
- Å E-mail used for transmitting trade secrets.
- Å IM messages lack security, can be easily intercept.

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 networkôs 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

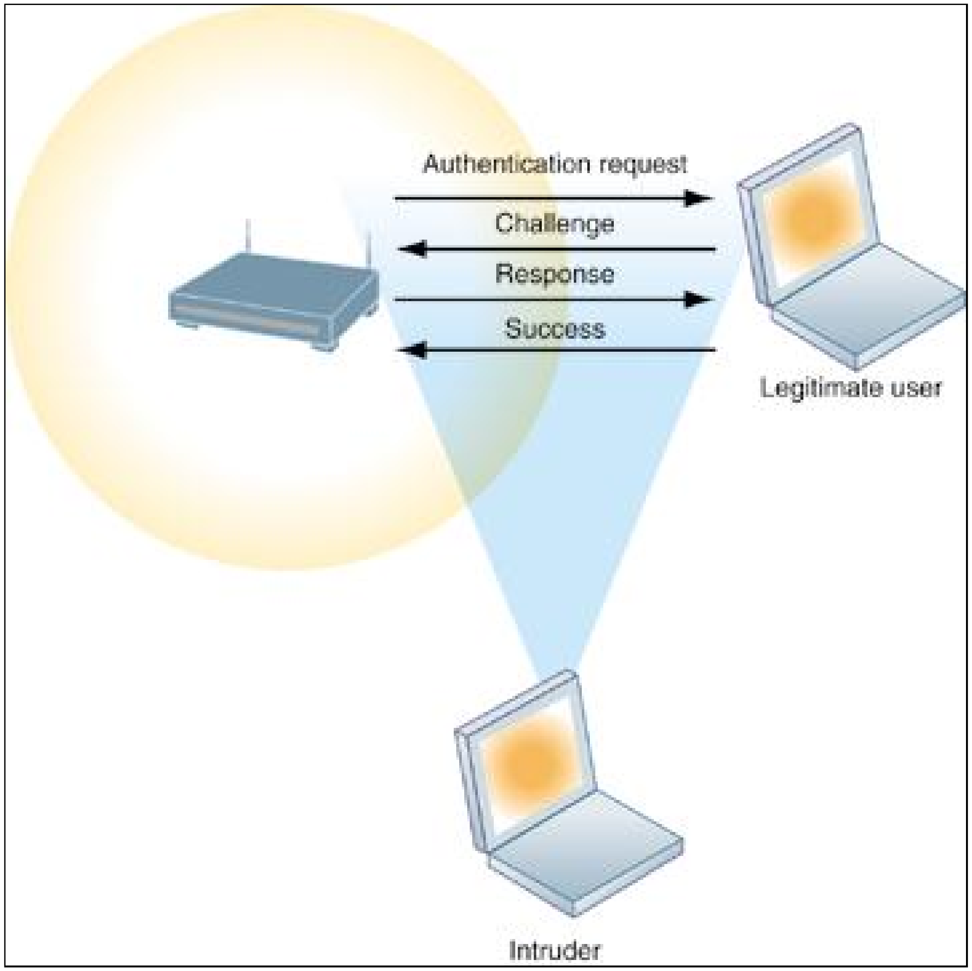


Figure 8-2

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.

System Vulnerability and Abuse

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

System Vulnerability and Abuse

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

Business Value of Security and Control

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

Establishing a Framework for Security and Control

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

Establishing a Framework for Security and Control

Å MIS audit

Å Examines firmŝ overall security environment as well as controls governing individual information systems

Å Reviews technologies, procedures, documentation, training, and personnel

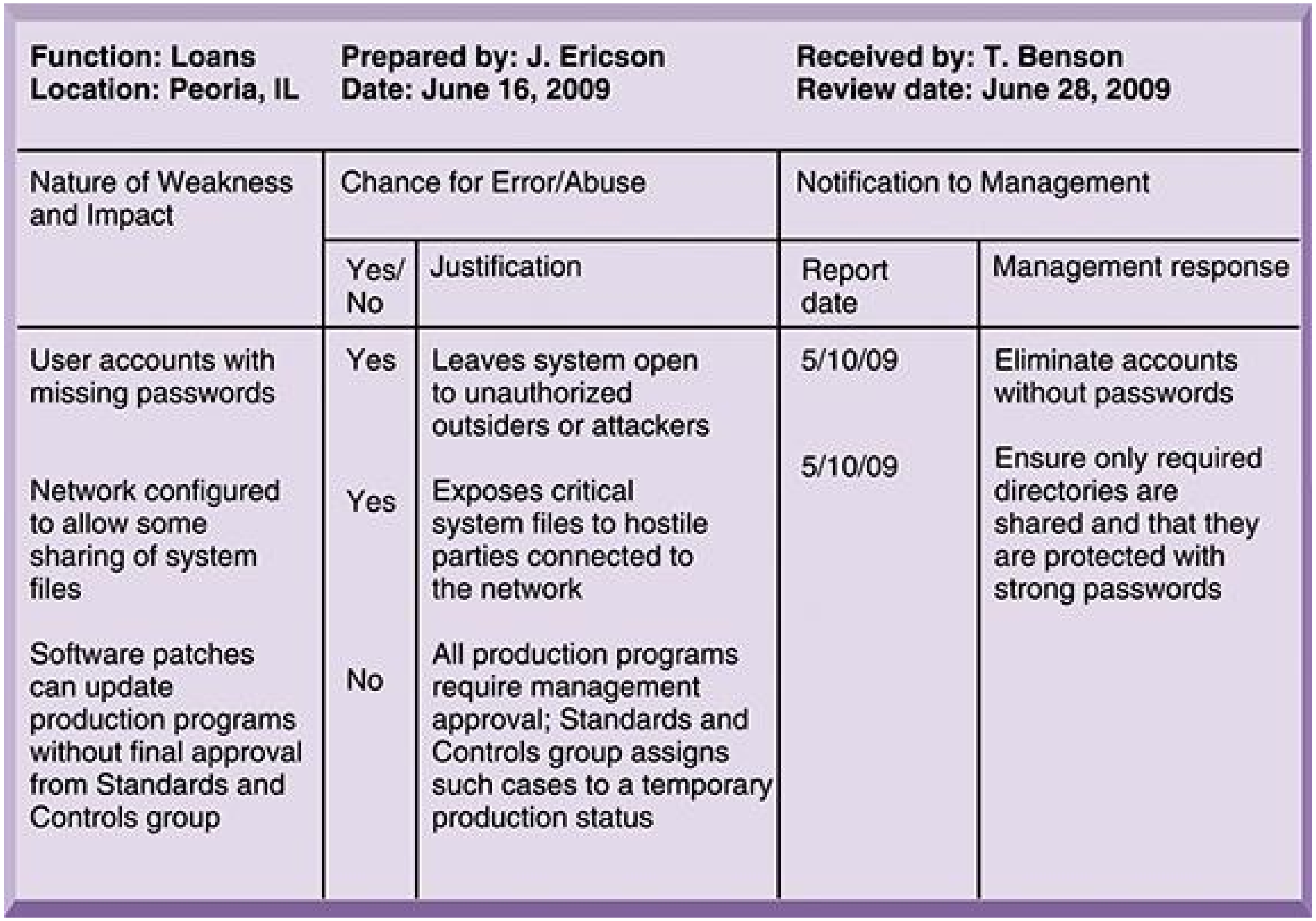
Å May even simulate disaster to test response of technology, IS staff, other employees

Å Lists and ranks all control weaknesses and estimates probability of their occurrence

Å Assesses financial and organizational impact of each threat

Establishing a Framework for Security and Control

Sample Auditor’s List of Control Weaknesses



Function: Loans
Location: Peoria, IL

Prepared by: J. Ericson
Date: June 16, 2009

Received by: T. Benson
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.