Chapter 7

Securing Information Systems

STUDENT OBJECTIVES

- Analyze why information systems need special protection from destruction, error, and abuse.
- Assess the business value of security and control.
- Design an organizational framework for security and control.
- Evaluate the most important tools and technologies for safeguarding information resources.

Phishing: A Costly New Sport for Internet Users

- Problem: Large number of vulnerable users of online financial services, ease of creating bogus Web sites.
- Solutions: Deploy anti-phishing software and services and a multilevel authentication system to identify threats and reduce phishing attempts.
- Deploying new tools, technologies, and security procedures, along with educating consumers, increases reliability and customer confidence.
- Demonstrates IT’s role in combating cyber crime.
- Illustrates digital technology as part of a multilevel solution as well as its limitations in overcoming discouraged consumers.

Phishing: A Costly New Sport for Internet Users

Interactive Session: Phishing

- Discuss suspicious e-mails that members of the class have received:
    - What made you suspicious of a particular e-mail?
    - Did you open the e-mail? Were there any consequences to this action?
    - Did you report the suspicious e-mail to anyone?
    - What measures have you taken to protect yourself from phishing scams?

System Vulnerability and Abuse

- **An unprotected computer connected to the Internet may be disabled within a few 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 the safety of the organization’s assets; the accuracy and reliability of its accounting records; and operational adherence to management standards**

System Vulnerability and Abuse

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, etc.)
- Internet vulnerabilities
- Wireless security challenges

Chapter 7 Securing Information Systems: System Vulnerability and Abuse

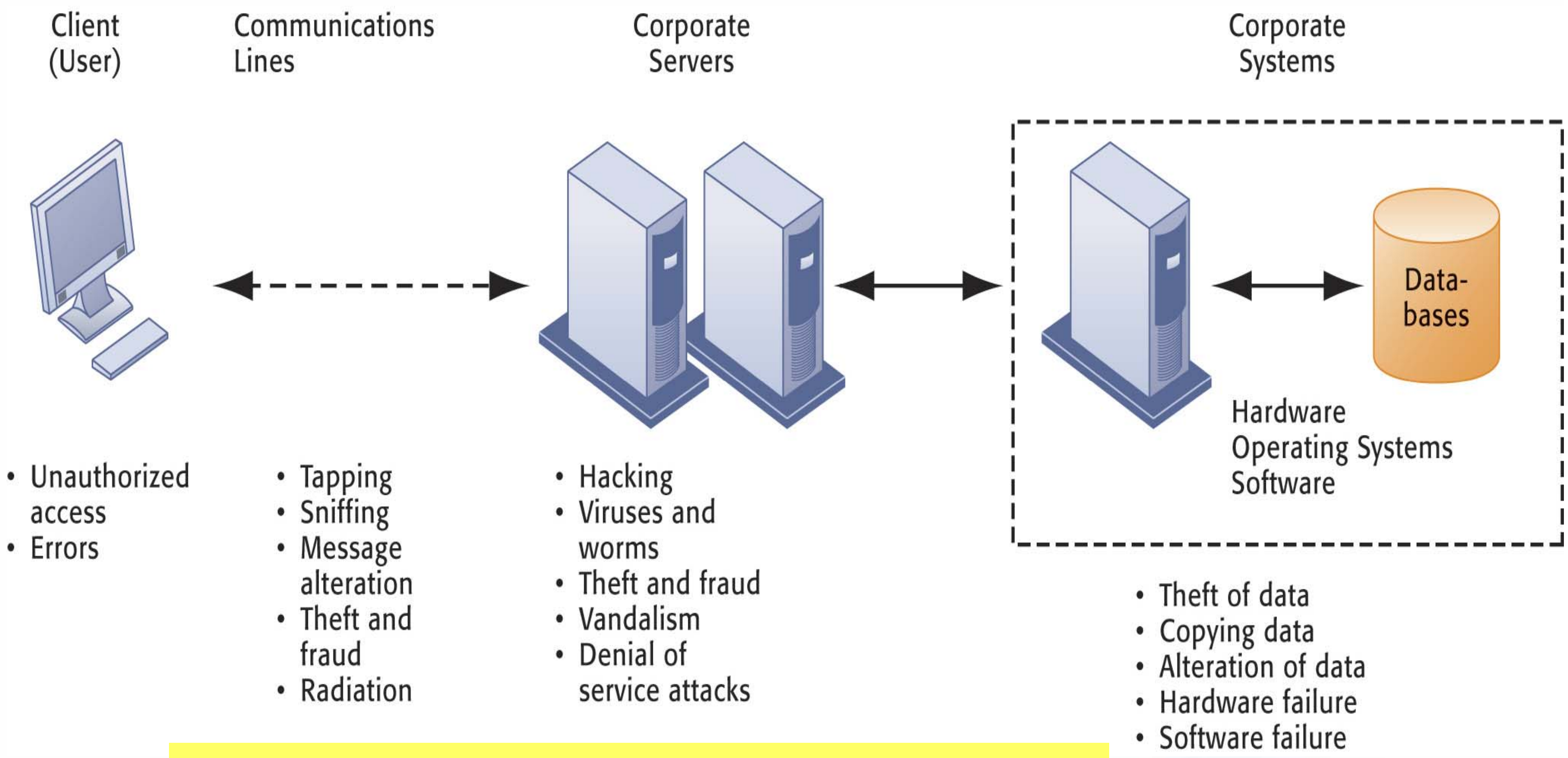


Figure 7-1, The Map of the Chapter

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

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

- **Malware**
  - **Viruses,** a virus is a program (a set of code) that replicates by being copied or initiating its copying to another program, computer boot sector or document.
  - **Worms** a self-replicating virus that does not alter files but **resides in active memory and duplicates itself.**
  - **Trojan horses** is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and execute its chosen form of damage, **such as ruining the file allocation table** on your hard disk.
  - **Spyware**
  - **Key loggers**

System Vulnerability and Abuse

Hackers and Cyber-vandalism

- **Hackers (** A hacker is an individual who intends to gain unauthorized access) **vs. crackers** (with ***criminal intent***)
- **Cyber-vandalism**
- **Spoofing** (misrepresenting, redirecting)
- **Sniffing** (eavesdropping to find weaknesses)
- **Denial-of-service (DoS) attack**
- **Distributed denial-of-service (DDoS) attack**

  (create numerous server request through many unauthorized servers (Botnet) to overwhelm the targeted server)
- **Botnets (**Zambie PC **-- software robots)**

Computer Crime and Cyberterrorism

- Computer crime: “any violations of criminal law that involve knowledge of computer technology for their perpetration, investigation, or prosecution” –U.S. Department of Justice
- U.S. companies lose $14 billion annually to cyber crime
- Cont’

System Vulnerability and Abuse

Identity theft :

Phishing, misrepresented Websites

evil twins, misrepresented hotspot

pharming, redirect to their Web page by gaining access to your IP address from ISP list

computer abuse: spamming:

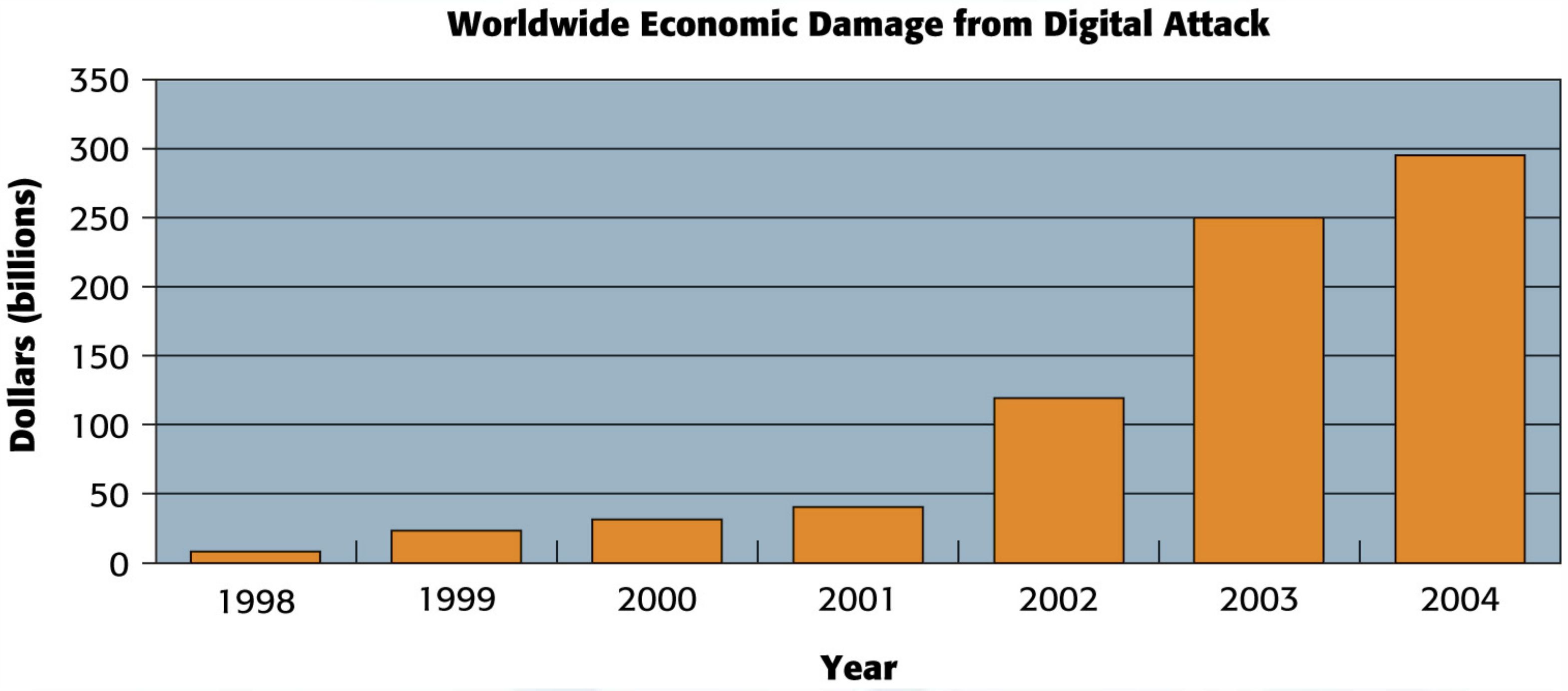
unsolicited, unethical not illegal)

Cyber-terrorism and cyber-warfare:

Attacks on computer-controlled system:

System Vulnerability and Abuse

Worldwide Damage from Digital Attacks



This chart shows estimates of the average worldwide damage from hacking, malware, and spam since 1998. These figures are based on data from mi2G and the authors.

Figure 7-3

System Vulnerability and Abuse

Internal Threats: Employees

- Security threats often originate inside an organization
  - Social engineering (colleague: getting one’s password)

Software Vulnerability

- Commercial software contains flaws that create security vulnerabilities
- Patches

Business Value of Security and Control

- Failed computer systems can lead to a significant or total loss of business function
- Firms are now more vulnerable than they have ever been
- 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

- **Electronic records management (ERM): policies, procedures, and tools for managing the retention, destruction, and storage of electronic records**
- **HIPAA (Health Insurance Portability and Accountability)**
- **Gramm-Leach-Bliley Act** ➔ **Financial Services Modernization**
- **Sarbanes-Oxley Act** ➔ Investor Protection Act

Electronic Evidence and Computer Forensics

- Evidence for legal actions often found in digital form
- Proper control of data can save money when responding to a discovery request
- Computer forensics: scientific collection, examination, authentication, preservation, and analysis of data from computer storage media for use as evidence in a court of law
- Ambient data (Hidden, background, ..) e.g. deleted files

Establishing a Framework for Security and Control

- ISO 17799
- Risk assessment
- Security policy
  - Chief security officer (CSO)
  - Acceptable use policy (AUP)
  - Authorization policies
  - Authorization management systems

Establishing a Framework for Security and Control

Ensuring Business Continuity

- Downtime
- Fault-tolerant computer systems
- High-availability computing
- Recovery-oriented computing
- Disaster recovery planning
- Business continuity planning
- Security outsourcing (managed security service providers)

Establishing a Framework for Security and Control

The Role of Auditing

- MIS audit
  - Identifies the controls that govern information systems and assesses their effectiveness
  - Auditor conducts interviews with key individuals
  - Examines security, application controls, overall integrity controls, and control disciplines

Technologies and Tools for Security

Access Control

- Authentication
  - Tokens
  - Smart cards hotel key, cash card
  - Biometric authentication

New Solutions for Identity Management

- Read the Focus on Technology and then discuss the following questions:
  - What problems were Monsanto, Clarian, and others having with identity management?
  - What was the impact of those problems?
  - What alternative solutions were available?
  - What people, organization, and technology issues had to be addressed in developing solutions?
  - Do you think the solutions chosen are effective? Why or why not?

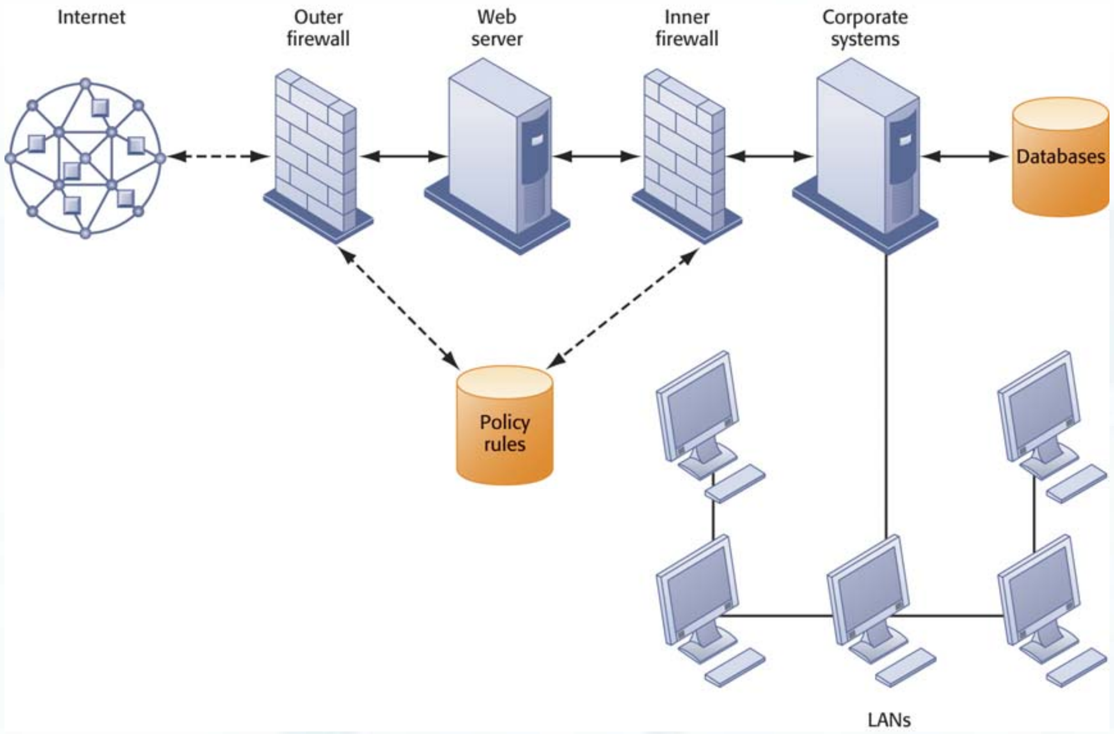
Technologies and Tools for Security

Firewalls, Intrusion Detection Systems, and Antivirus Software

- **Firewall: a combination of hardware and software that prevents unauthorized users from accessing private networks**
- **Intrusion detection systems monitor hot spots on corporate networks to detect and deter intruders**
- **Antivirus and antispyware software checks computers for the presence of malware and can often eliminate it as well**

Technologies and Tools for Security

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 7-6

Technologies and Tools for Security

Securing Wireless Networks

- WEP security can be improved by using it with VPN technology
- Wi-Fi Alliance/Wi-Fi Protected Access (WPA) specifications
- Extensible Authentication Protocol (EAP)
- Protection from rogue networks

Technologies and Tools for Security

Interactive Session: Securing Wireless Networks

- Do you use wireless technology?
- If so, what kinds of information do you transmit over the wireless network?
- What kinds of information do you avoid sending over the wireless network? What are your concerns related to sending these kinds of information?
- If you do not have access to a wireless network, is it by choice due to security concerns?

Encryption and Public Key Infrastructure

- Encryption: transforming text or data into cipher text that cannot be read by unintended recipients
  - Secure Sockets Layer (SSL)
  - Transport Layer Security (TLS)
  - Secure Hypertext Transfer Protocol (S-HTTP)
  - Public key encryption
  - Digital signature
  - Digital certificate
  - Public key infrastructure (PKI)