Securing Information Systems

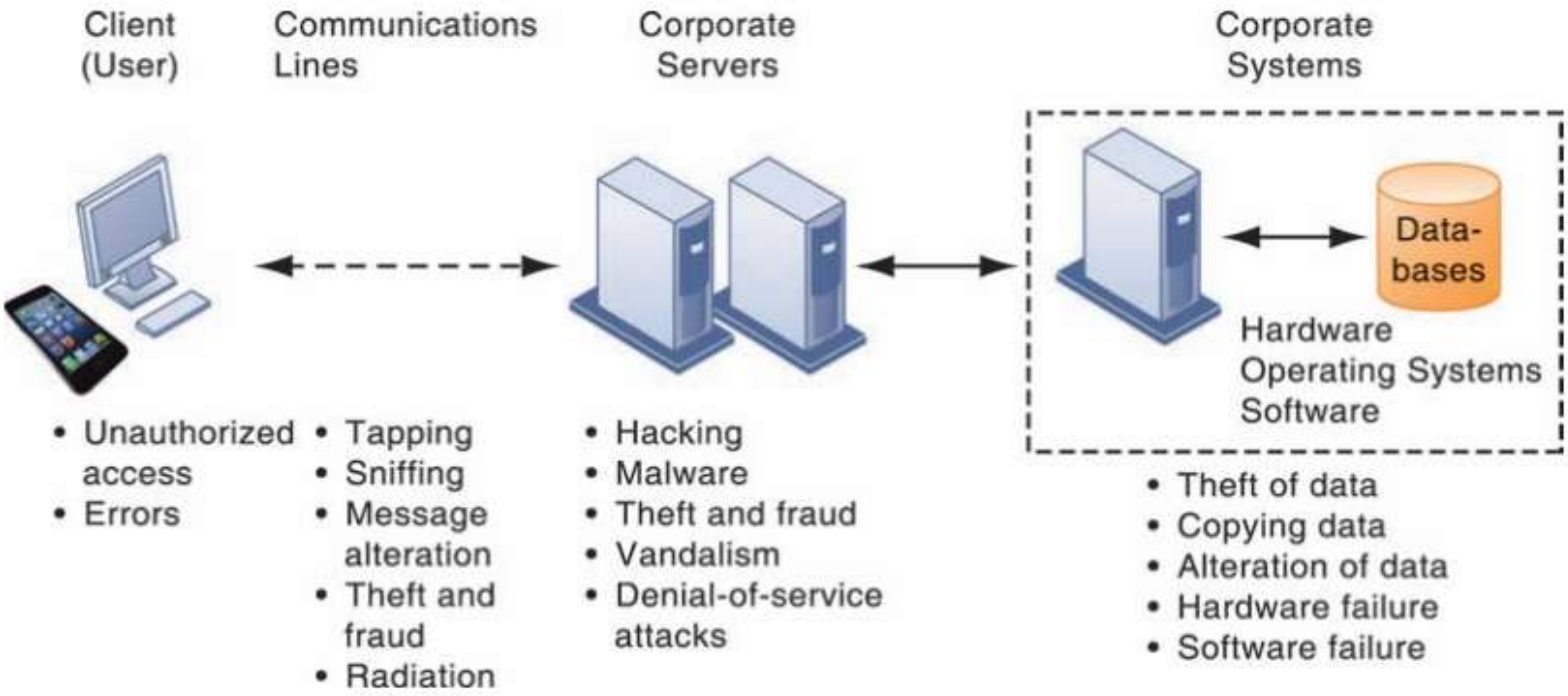
Why are information systems vulnerable to destruction, error, and abuse?

- if you operate a business today, you need to make security and control a top priority.
- Security refers to the policies, procedures, and technical measures used to prevent unauthorized access, alteration, theft, or physical damage to information systems.

Why Systems are Vulnerable

- The potential for unauthorized access, abuse, or fraud is not limited to a single location but can occur at any access point in the network.

FIGURE 8.1 CONTEMPORARY SECURITY CHALLENGES AND VULNERABILITIES



Client (User)

- Unauthorized access
- Errors

Communications Lines

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

Corporate Servers

- Hacking
- Malware
- Theft and fraud
- Vandalism
- Denial-of-service attacks

Corporate Systems

Data- bases

Hardware
Operating Systems
Software

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

Malicious software

- Malicious software programs are referred to as malware and include a variety of threats such as computer viruses, worms, and Trojan horses.

Computer virus

- computer virus is a software program that attaches itself to other software programs or data files to be executed, usually without user knowledge or permission.

worms

- which are independent computer programs that copy themselves from one computer to other computers over a network.
- Worms can operate on their own without attaching to other computer program files and rely less on human behavior to spread from computer to computer.

- Worms and viruses are often spread over the Internet
  - from files of downloaded software;
  - from files attached to e-mail transmissions;
  - from compromised e-mail messages
  - online ads
  - instant messaging.

Trojan horse

- A software program that appears to be benign but then does something other than expected.
- It is often a way for viruses or other malicious code to be introduced into a computer system.
- It is often used to steal login credentials for banking by surreptitiously capturing people’s keystrokes as they use their computers.

SQL injection

- These vulnerabilities occur when a web application fails to validate properly or filter data a user enters on a web page, which might occur when ordering something online.
- An attacker uses this input validation error to send a rogue SQL query to the underlying database to access the database, plant malicious code, or access other systems on the network.

spyware

- Spyware is loosely defined as **malicious software** designed to enter your computer device, gather data about you, and forward it to a third-party without your consent.
- Spyware can also refer to legitimate software that monitors your data for commercial purposes like advertising.

Hackers and computer crime

- A hacker is an individual who intends to gain unauthorized access to a computer system.
- Hackers gain unauthorized access by finding weaknesses in the security protections websites and computer systems employ, often taking advantage of various features of the Internet that make it an open system and easy to use.

Spoofing and sniffing

- Hackers attempting to hide their true identities often spoof, or misrepresent, themselves by using fake e-mail addresses
- Spoofing may also involve redirecting a web link to an address different from the intended one,
  - For example, if hackers redirect customers to a fake website that looks almost exactly like the true site, they can then collect and process orders, effectively stealing business as well as sensitive customer information from the true site

- A sniffer is a type of eavesdropping program that monitors information traveling over a network.
- sniffers help identify potential network trouble spots or criminal activity on networks, but when used for criminal purposes, they can be damaging and very difficult to detect.
- Sniffers enable hackers to steal proprietary information from anywhere on a network, including e-mail messages, company files, and confidential rep

Denial-of-Service

- Denial-of-Service Attacks In a denial-of-service (DoS) attack, hackers flood a network server or web server with many thousands of false communications or requests for services to crash the network.
- The network receives so many queries that it cannot keep up with them and is thus unavailable to service legitimate requests. A distributed denial-of-service (DDoS) attack uses numerous computers to inundate and overwhelm the network from numerous launch points.

Identity Theft

- With the growth of the Internet and electronic commerce, identity theft has become especially troubling.
- Identity theft is a crime in which an imposter obtains key pieces of personal information, such as social security numbers, driver’s license numbers, or credit card numbers, to impersonate someone else.
- The information may be used to obtain credit, merchandise, or services in the name of the victim or to provide the thief with false credentials.

phishing

- One increasingly popular tactic is a form of spoofing called phishing.
- Phishing involves setting up fake websites or sending e-mail messages that look like those of legitimate businesses to ask users for confidential personal data.
- The e-mail message instructs recipients to update or confirm records by providing social security numbers, bank and credit card information, and other confidential data either by responding to the e-mail message, by entering the information at a bogus website, or by calling a telephone number.

WHAT ARE THE MOST IMPORTANT TOOLS AND TECHNOLOGIES FOR SAFEGUARDING INFORMATION RESOURCES?

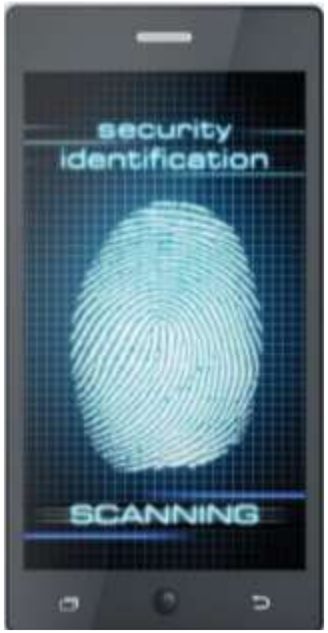
Identity Management and Authentication

- all users and their system privileges, assigning each user a unique digital identity for accessing each system.
- It also includes tools for authenticating users, protecting user identities, and controlling access to system resources.

Authentication..

- To gain access to a system, a user must be authorized and authenticated. Authentication refers to the ability to know that a person is who he or she claims to be.
- Authentication is often established by using passwords known only to authorized users.

- New authentication technologies, such as tokens, smart cards, and biometric authentication, overcome some of these problems



Firewalls, Intrusion Detection Systems, and Antivirus Software

- Without protection against malware and intruders, connecting to the Internet would be very dangerous.
- Firewalls, intrusion detection systems, and antivirus software have become essential business tools.

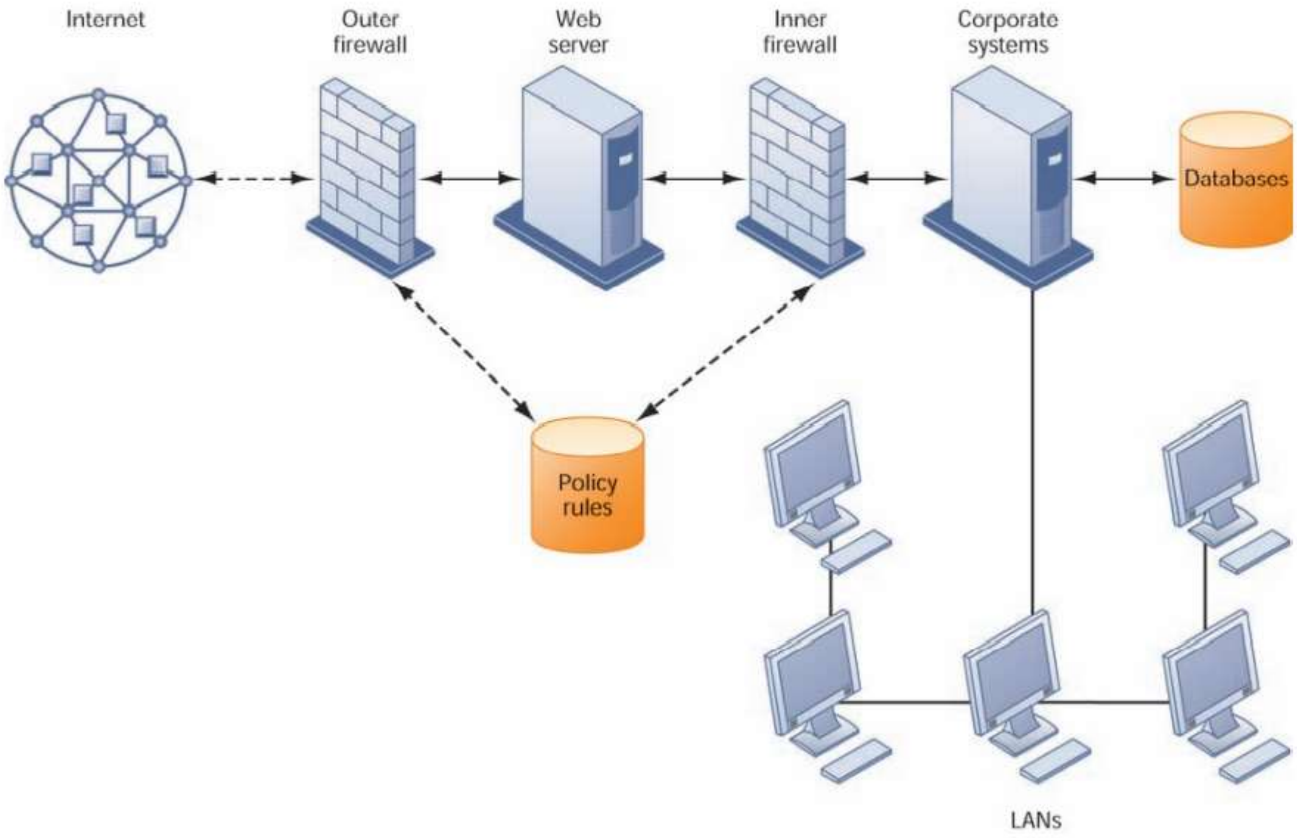
Firewalls

- Firewalls prevent unauthorized users from accessing private networks.
- It is a combination of hardware and software that controls the flow of incoming and outgoing network traffic.
- It is generally placed between the organization’s private internal networks and external networks, such as the Internet, although firewalls can also be used to protect one part of a company’s network from the rest of the network .

Firewalls..

- It checks this information against the access rules that the network administrator has programmed into the system. The firewall prevents unauthorized communication into and out of the network.
- There are a number of firewall screening technologies, including
  - static packet filtering,
  - stateful inspection
  - Network Address Translation
  - application proxy filtering.
- They are frequently used in combination to provide firewall protection.

FIGURE 8.5 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.

Intrusion Detection Systems

- Intrusion detection systems feature full-time monitoring tools placed at the most vulnerable points or hot spots of corporate networks to detect and deter intruders continually.
- The system generates an alarm if it finds a suspicious or anomalous event.
- Scanning software looks for patterns indicative of known methods of computer attacks such as bad passwords, checks to see whether important files have been removed or modified, and sends warnings of vandalism or system administration errors.
- The intrusion detection tool can also be customized to shut down a particularly sensitive part of a network if it receives unauthorized traffic.

- Antivirus and Antispyware Software Defensive technology plans for both individuals and businesses must include anti-malware protection for every computer.
- Antivirus software prevents, detects, and removes malware, including computer viruses, computer worms, Trojan horses, spyware, and adware.

Threat Management Systems

- Unified Threat Management Systems To help businesses reduce costs and improve manageability, security vendors have combined into a single appliance various security tools, including firewalls, virtual private networks, intrusion detection systems, and web content filtering and anti-spam software.
- These comprehensive security management products are called unified threat management (UTM) systems.
- UTM products are available for all sizes of networks. Leading UTM vendors include Fortinent, Sophos, and Check Point, and networking vendors such as Cisco Systems and Juniper Networks provide some UTM capabilities in their products.

WHAT ARE THE COMPONENTS OF AN ORGANIZATIONAL FRAMEWORK FOR SECURITY AND CONTROL?

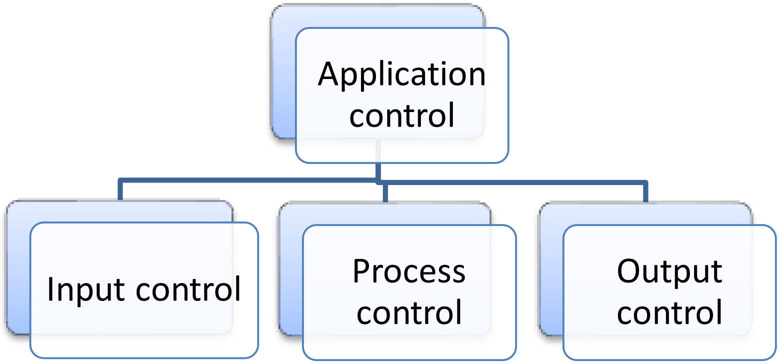
Information System Controls

General control

- General controls include
  - software controls
  - physical hardware controls
  - computer operations controls
  - data security controls
  - controls over the systems development process,
  - administrative controls.

Application controls

- Application controls are specific controls unique to each computerized application, such as payroll or order processing.



Input controls check data for accuracy and completeness There are specific input controls for input authorization, data conversion, data editing, and error handling

Processing controls establish that data are complete and accurate during updating

Output controls ensure that the results of computer processing are accurate, complete, and properly distributed

Risk assessment

- A risk assessment determines the level of risk to the firm if a specific activity or process is not properly controlled.
- After the risks have been assessed, system builders will concentrate on the control points with the greatest vulnerability and potential for loss

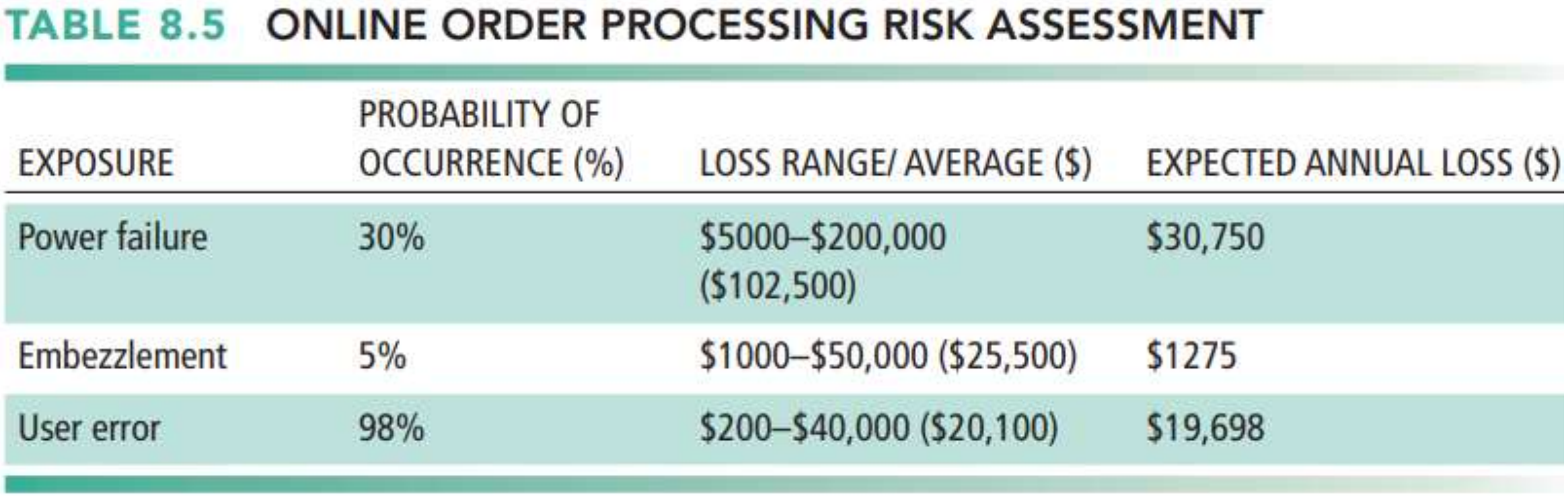


TABLE 8.5 ONLINE ORDER PROCESSING RISK ASSESSMENT

EXPOSURE	PROBABILITY OF OCCURRENCE (%)	LOSS RANGE/ AVERAGE ($)	EXPECTED ANNUAL LOSS ($)
Power failure	30%	$5000–$200,000 ($102,500)	$30,750
Embezzlement	5%	$1000–$50,000 ($25,500)	$1275
User error	98%	$200–$40,000 ($20,100)	$19,698

Security Policy

- After you’ve identified the main risks to your systems, your company will need to develop a security policy for protecting the company’s assets.

- A security policy consists of statements
  - ranking information risks
  - identifying acceptable security goals
  - identifying the mechanisms for achieving these goals.

Disaster Recovery Planning and Business Continuity Planning

- Disaster recovery planning devises plans for the restoration of disrupted computing and communications services.

The Role of Auditing

- An information systems audit examines the firm’s overall security environment as well as controls governing individual information systems.
- Security audits review technologies, procedures, documentation, training, and personnel.

END