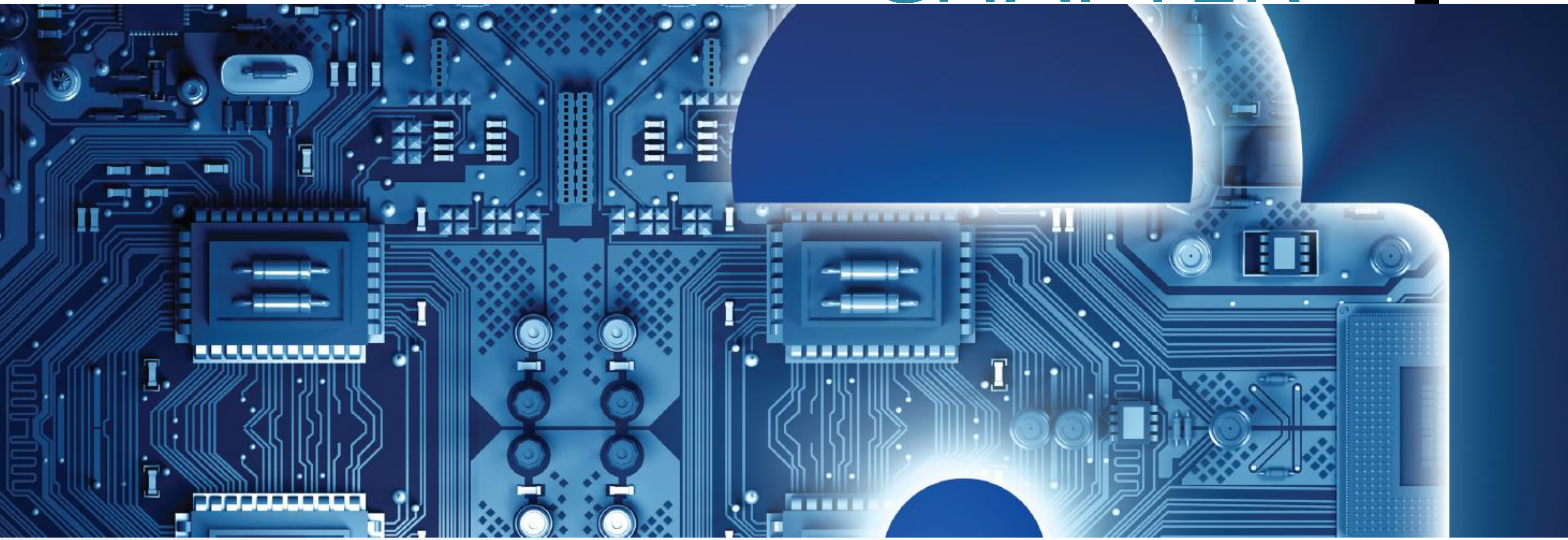
CHAPTER 7



Information Security

CHAPTER OUTLINE

1. Introduction to Information Security
2. Unintentional Threats to Information Systems
3. Deliberate Threats to Information Systems
4. What Organizations Are Doing to Protect Information Resources
5. Information Security Controls

LEARNING OBJECTIVES

1. Identify the five factors that contribute to the increasing vulnerability of information resources and specific examples of each factor.
2. Compare and contrast human mistakes and social engineering, along with specific examples of each one.
3. Discuss the 10 types of deliberate attacks.
4. Describe the three risk mitigation strategies and examples of each one in the context of owning a home.
5. Identify the three major types of controls that organizations can use to protect their information resources along with an example of each one.

7.1 Introduction to Information Security

- Security
  - the degree of protection against criminal activity, danger, damage, and/or loss.
- Information Security
  - all of the processes and policies designed to protect an organization’s information and information systems (IS) from unauthorized access, use, disclosure, disruption, modification, or destruction.
- Threat
  - any danger to which a system may be exposed.
- Exposure
  - of an information resource is the harm, loss, or damage that can result if a threat compromises that resource.
- Vulnerability
  - the possibility that the system will be harmed by a threat.
- Cybercrime
  - refers to illegal activities conducted over computer networks, particularly the Internet. iDefense (http://labs.idefense.com), a company that specializes in providing security information to governments and Fortune 500 companies, maintains that groups of well-organized criminal organizations have taken control of a global billiondollar crime network.

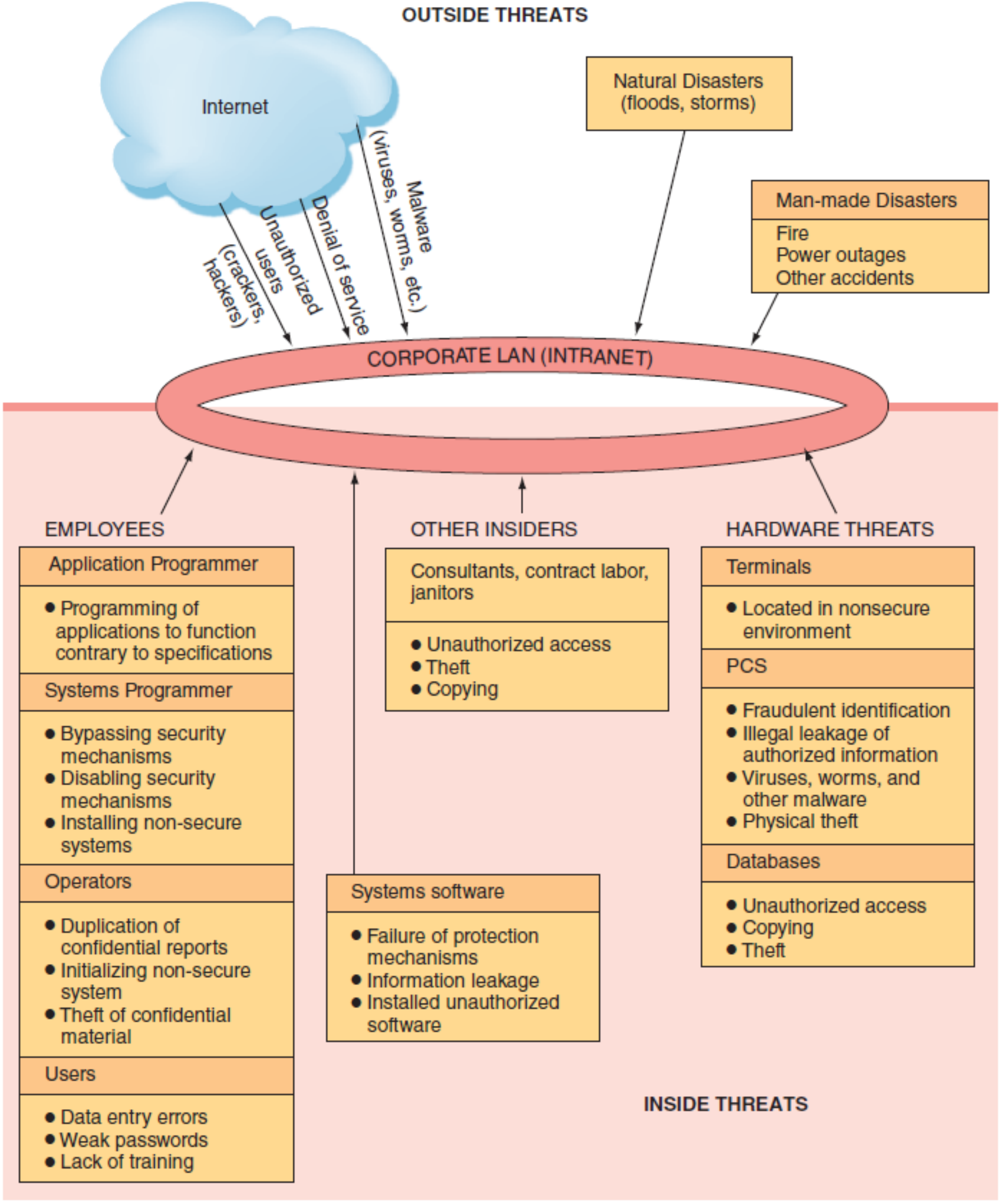
Five Key Factors Increasing Vulnerability

1. Today’s interconnected, interdependent, wirelessly networked business environment
2. Smaller, faster, cheaper computers and storage devices
3. Decreasing skills necessary to be a computer hacker
4. International organized crime taking over cybercrime
5. Lack of management support

7.2 Unintentional Threats to Information Systems

- Human Errors
- Social Engineering

Figure 7.1 Security Threats



OUTSIDE THREATS

Internet

Natural Disasters (floods, storms)

Man-made Disasters

Fire
Power outages
Other accidents

Unauthorized users (crackers, hackers)

Denial of service

Malware (viruses, worms, etc.)

CORPORATE LAN (INTRANET)

EMPLOYEES

Application Programmer

- Programming of applications to function contrary to specifications

Systems Programmer

- Bypassing security mechanisms
- Disabling security mechanisms
- Installing non-secure systems

Operators

- Duplication of confidential reports
- Initializing non-secure system
- Theft of confidential material

Users

- Data entry errors
- Weak passwords
- Lack of training

OTHER INSIDERS

Consultants, contract labor, janitors

- Unauthorized access
- Theft
- Copying

Systems software

- Failure of protection mechanisms
- Information leakage
- Installed unauthorized software

HARDWARE THREATS

Terminals

- Located in nonsecure environment

PCS

- Fraudulent identification
- Illegal leakage of authorized information
- Viruses, worms, and other malware
- Physical theft

Databases

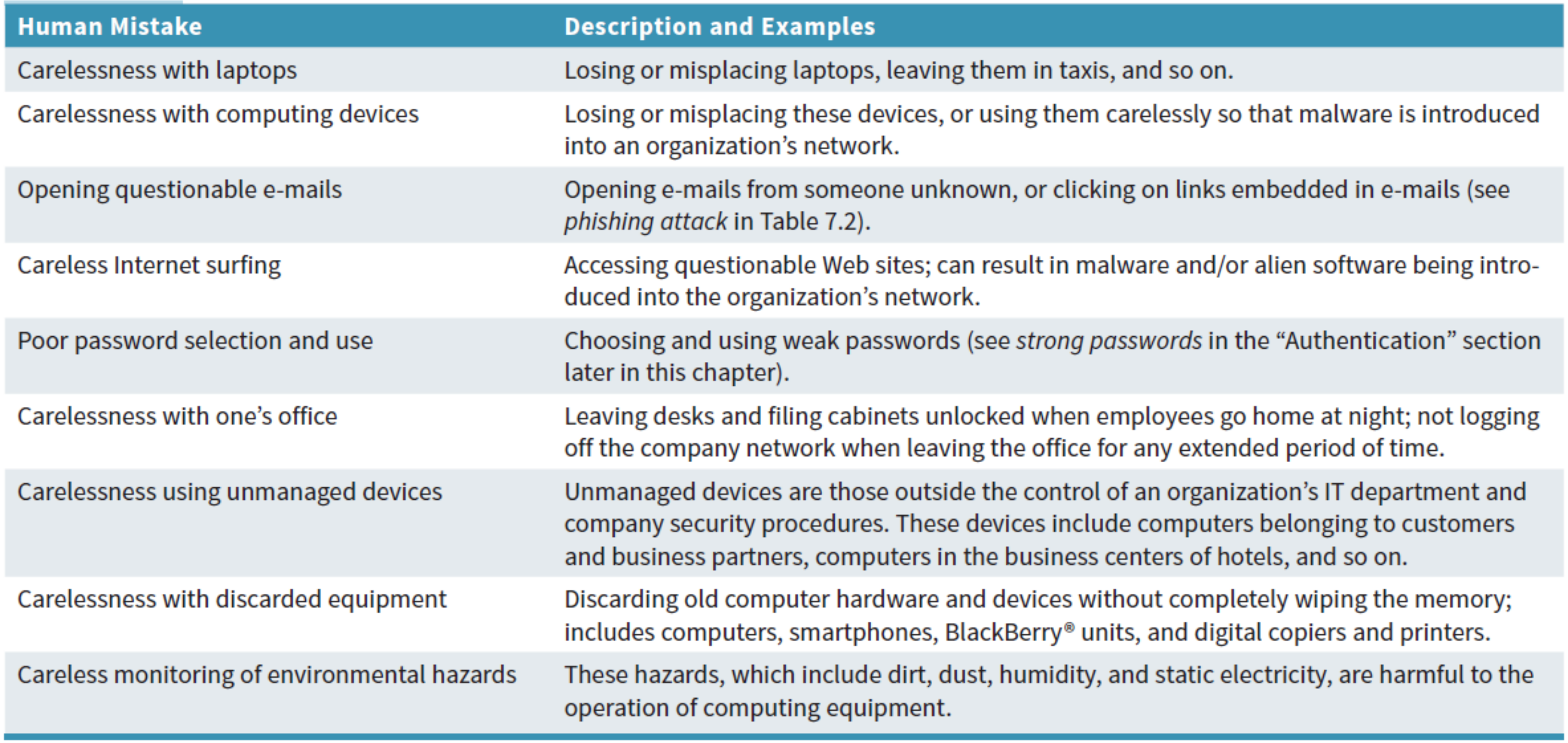
- Unauthorized access
- Copying
- Theft

INSIDE THREATS

Human Errors

- Higher employee levels = higher levels of security risk
  - This is true because higher-level employees typically have greater access to corporate data, and they enjoy greater privileges on organizational information systems.
- Most Dangerous Employees
  - Two organizational areas pose the greatest risk
    - Human Resources
      - Human resources employees generally have access to sensitive personal information about all employees.
    - Information Systems
      - IS employees not only have access to sensitive organizational data, but also often control the means to create, store, transmit, and modify those data.
- Janitors and Guards Frequently Overlooked
  - Companies frequently outsource their security and janitorial services.

Table 7.1: Human Mistakes



Human Mistake	Description and Examples
Carelessness with laptops	Losing or misplacing laptops, leaving them in taxis, and so on.
Carelessness with computing devices	Losing or misplacing these devices, or using them carelessly so that malware is introduced into an organization’s network.
Opening questionable e-mails	Opening e-mails from someone unknown, or clicking on links embedded in e-mails (see *phishing attack* in Table 7.2).
Careless Internet surfing	Accessing questionable Web sites; can result in malware and/or alien software being introduced into the organization’s network.
Poor password selection and use	Choosing and using weak passwords (see *strong passwords* in the “Authentication” section later in this chapter).
Carelessness with one’s office	Leaving desks and filing cabinets unlocked when employees go home at night; not logging off the company network when leaving the office for any extended period of time.
Carelessness using unmanaged devices	Unmanaged devices are those outside the control of an organization’s IT department and company security procedures. These devices include computers belonging to customers and business partners, computers in the business centers of hotels, and so on.
Carelessness with discarded equipment	Discarding old computer hardware and devices without completely wiping the memory; includes computers, smartphones, BlackBerry® units, and digital copiers and printers.
Careless monitoring of environmental hazards	These hazards, which include dirt, dust, humidity, and static electricity, are harmful to the operation of computing equipment.

Social Engineering

- **Social Engineering:**
  - an attack in which the perpetrator uses social skills to trick or manipulate legitimate employees into providing confidential company information such as passwords.
  - The most common example of social engineering occurs when the attacker impersonates someone else on the telephone, such as a company manager or an information systems employee. The attacker claims he forgot his password and asks the legitimate employee to give him a password to use.

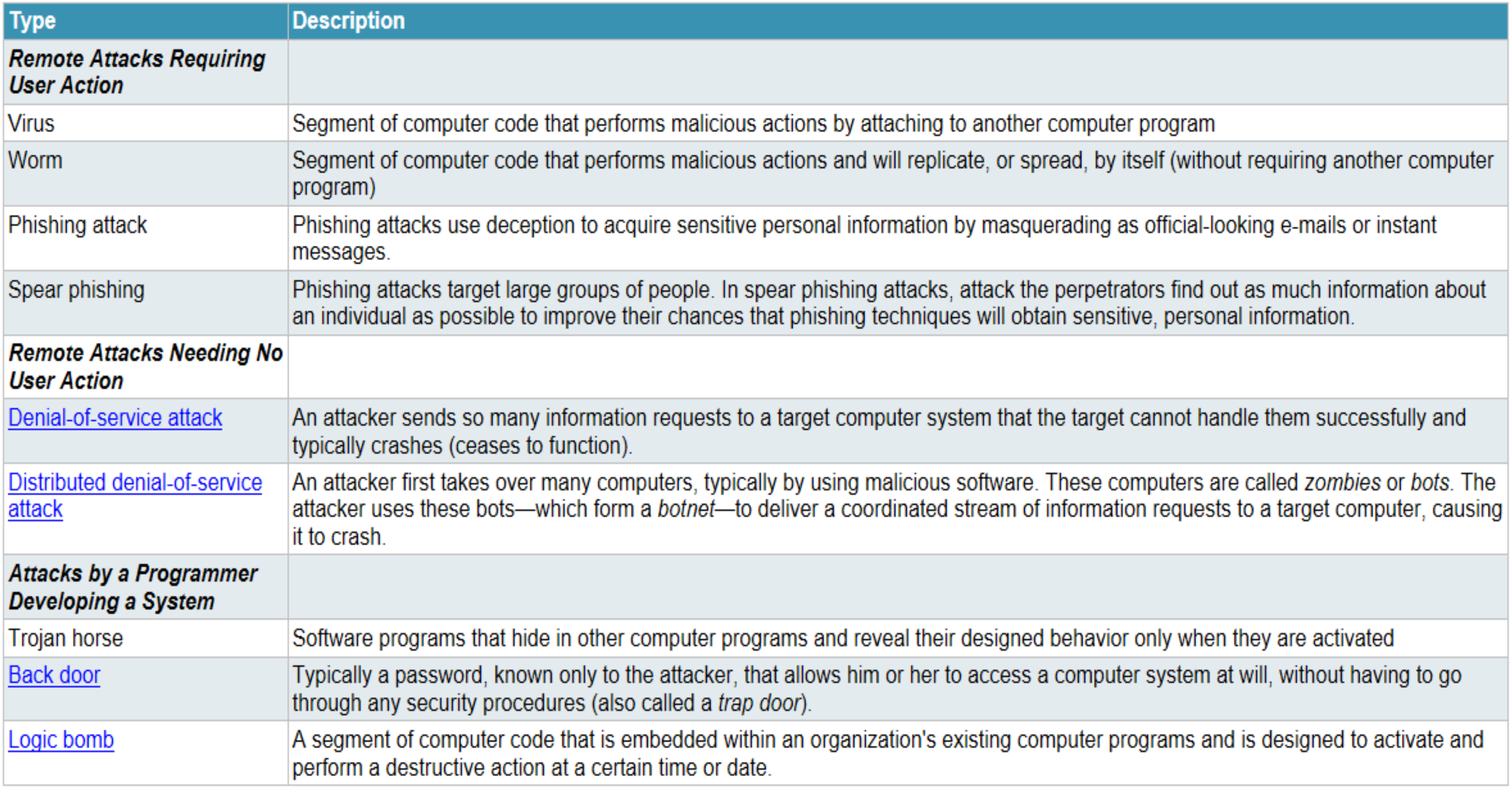
7.3 Deliberate Threats to Information Systems

1. Espionage or Trespass
   - occurs when an unauthorized individual attempts to gain illegal access to organizational information.
2. Information Extortion
   - occurs when an attacker either threatens to steal, or actually steals, information from a company. The perpetrator demands payment for not stealing the information, for returning stolen information, or for agreeing not to disclose the information.
3. Sabotage or Vandalism
   - deliberate acts that involve defacing an organization’s Web site, potentially damaging the organization’s image and causing its customers to lose faith.
   - One form of online vandalism is a hacktivist or cyberactivist operation.
4. Theft of Equipment or Information
   - Computing devices and storage devices are becoming smaller yet more powerful with vastly increased storage and as a result these devices are becoming easier to steal and easier for attackers to use to steal information.
   - One form of theft, known as dumpster diving, involves rummaging through commercial or residential trash to find discarded information. Paper files, letters, memos, photographs, IDs, passwords, credit cards, and other forms of information can be found in dumpsters.

7.3 Deliberate Threats to Information Systems

5. Identity Theft
   - is the deliberate assumption of another person's identity, usually to gain access to his or her financial information or to frame him or her for a crime.
6. Compromises to Intellectual Property
   - **Trade Secret:** an intellectual work, such as a business plan, that is a company secret and is not based on public information.
   - **Patent:** an official document that grants the holder exclusive rights on an invention or a process for a specified period of time.
   - **Copyright:** a statutory grant that provides the creators or owners of intellectual property with ownership of the property, also for a designated period.
   - **Intellectual Property:** the property created by individuals or corporations that is protected under trade secret, patent, and copyright laws.
7. Software Attacks
   - attackers used malicious software (called **malware**) to infect as many computers worldwide as possible, to the profit-driven,

7.3 Table 7.2 Type of Software Attacks



Type	Description
Remote Attacks Requiring User Action	
Virus	Segment of computer code that performs malicious actions by attaching to another computer program
Worm	Segment of computer code that performs malicious actions and will replicate, or spread, by itself (without requiring another computer program)
Phishing attack	Phishing attacks use deception to acquire sensitive personal information by masquerading as official-looking e-mails or instant messages.
Spear phishing	Phishing attacks target large groups of people. In spear phishing attacks, attack the perpetrators find out as much information about an individual as possible to improve their chances that phishing techniques will obtain sensitive, personal information.
Remote Attacks Needing No User Action	
Denial-of-service attack	An attacker sends so many information requests to a target computer system that the target cannot handle them successfully and typically crashes (ceases to function).
Distributed denial-of-service attack	An attacker first takes over many computers, typically by using malicious software. These computers are called *zombies* or *bots*. The attacker uses these bots—which form a *botnet*—to deliver a coordinated stream of information requests to a target computer, causing it to crash.
Attacks by a Programmer Developing a System	
Trojan horse	Software programs that hide in other computer programs and reveal their designed behavior only when they are activated
Back door	Typically a password, known only to the attacker, that allows him or her to access a computer system at will, without having to go through any security procedures (also called a *trap door*).
Logic bomb	A segment of computer code that is embedded within an organization's existing computer programs and is designed to activate and perform a destructive action at a certain time or date.

7.3 Deliberate Threats to Information Systems (continued)

9. Supervisory Control and Data Acquisition Attacks
   - refers to a large-scale, distributed measurement and control system. SCADA systems are used to monitor or to control chemical, physical, and transport processes such as those used in oil refineries, water and sewage treatment plants, electrical generators, and nuclear power plants.
   - If attackers gain access to the network, they can cause serious damage, such as disrupting the power grid over a large area or upsetting the operations of a large chemical or nuclear plant. Such actions could have catastrophic results.
10. Cyberterrorism and Cyberwarfare
   - refer to malicious acts in which attackers use a target’s computer systems, particularly via the Internet, to cause physical, real-world harm or severe disruption, often to carry out a political agenda.

7.3 Deliberate Threats to Information Systems (continued)

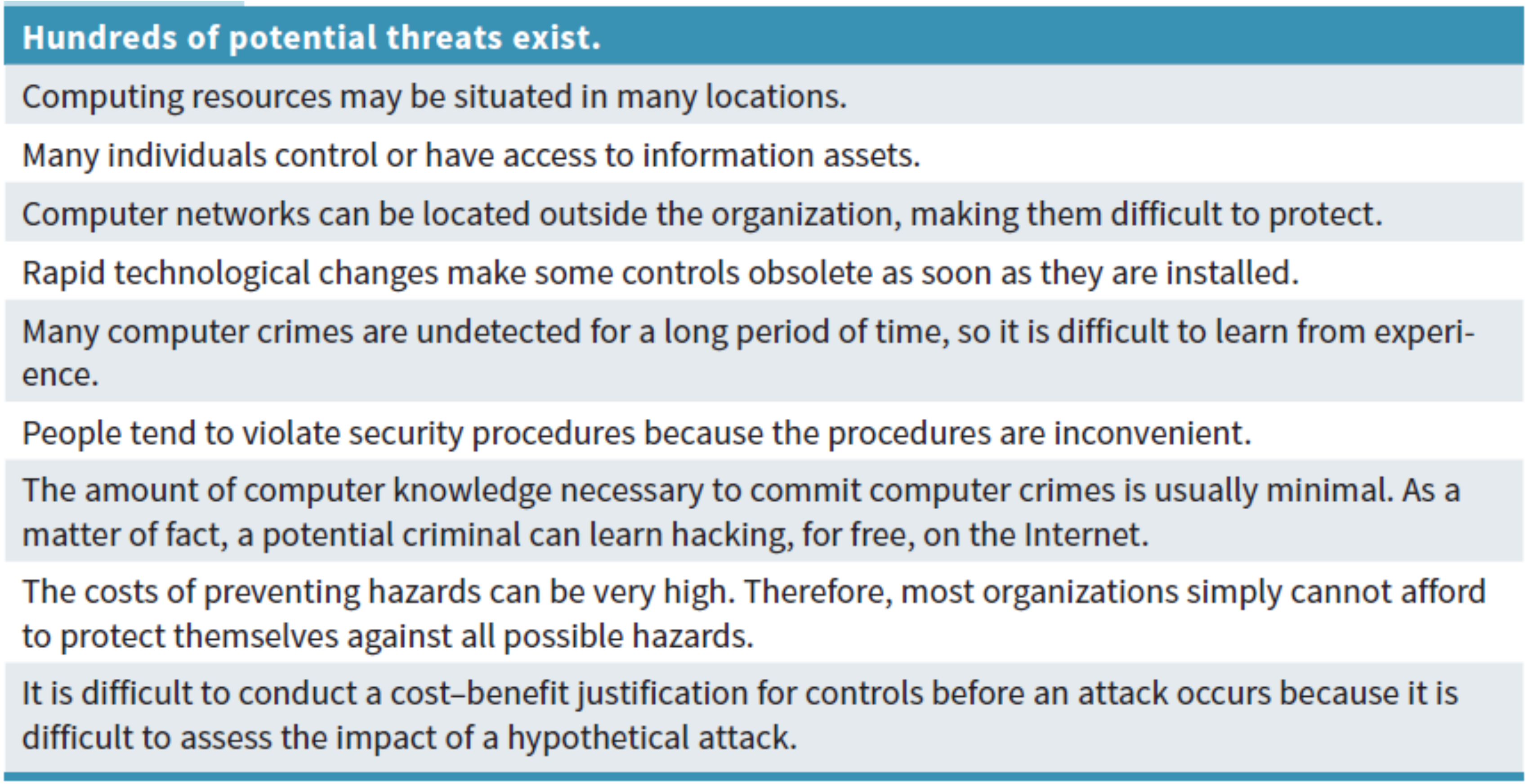
8. Alien Software

- secret software that is installed on your computer through duplicitous methods.
- it does use up valuable system resources. In addition, it can enable other parties to track your Web surfing habits and other personal behaviors.
- Adware :
  - software that causes pop-up advertisements to appear on your screen.
- Spyware :
  - software that collects personal information about users without their consent.
  - keystroke loggers and screen scrapers.
- Spamware :
  - pestware that uses your computer as a launch pad for spammers

7.4 What Organizations Are Doing to Protect Information Resources

- Risk
- Risk Management
- Risk Analysis
- Risk Mitigation

Table 7.3: The Difficulties in Protecting Information Resources



Hundreds of potential threats exist.
Computing resources may be situated in many locations.
Many individuals control or have access to information assets.
Computer networks can be located outside the organization, making them difficult to protect.
Rapid technological changes make some controls obsolete as soon as they are installed.
Many computer crimes are undetected for a long period of time, so it is difficult to learn from experience.
People tend to violate security procedures because the procedures are inconvenient.
The amount of computer knowledge necessary to commit computer crimes is usually minimal. As a matter of fact, a potential criminal can learn hacking, for free, on the Internet.
The costs of preventing hazards can be very high. Therefore, most organizations simply cannot afford to protect themselves against all possible hazards.
It is difficult to conduct a cost–benefit justification for controls before an attack occurs because it is difficult to assess the impact of a hypothetical attack.

Risk Management

Risk Management:

identifies, controls, and minimizes the impact of threats. In other words, risk management seeks to reduce risk to acceptable levels.

Three Processes of Risk Management:

1. risk analysis
2. risk mitigation
3. controls evaluation

Risk Analysis

Three Steps of Risk Analysis

1. assessing the value of each asset being protected
2. estimating the probability that each asset will be compromised
3. comparing the probable costs of the asset’s being compromised with the costs of protecting that asset

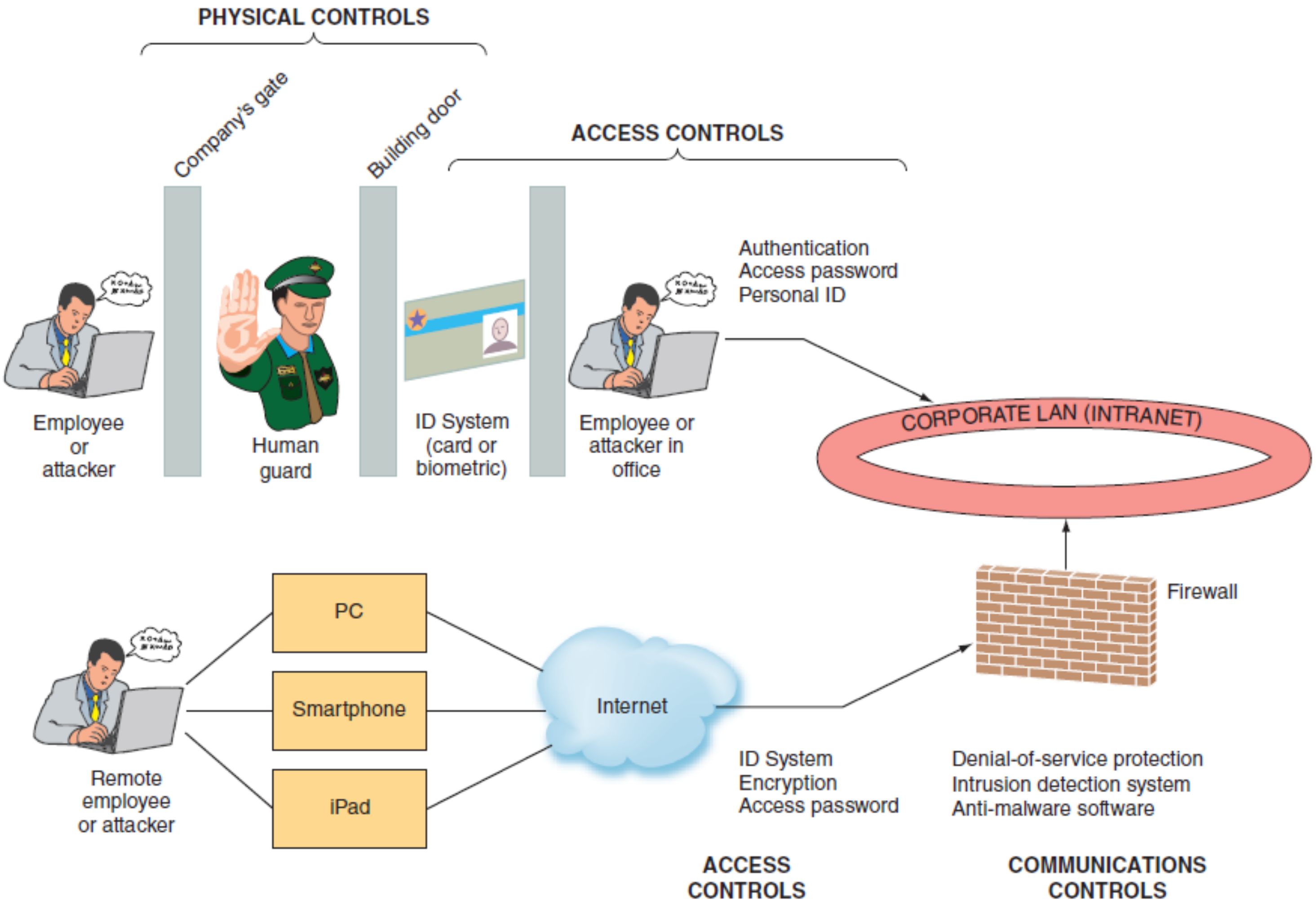
Risk Mitigation

- **Risk Mitigation:**
  - the organization takes concrete actions against risks which has two functions:
  - Two functions
    1. implementing controls to prevent identified threats from occurring
    2. developing a means of recovery if the threat becomes a reality
- Risk Mitigation Strateges
  - Risk Acceptance
    - Accept the potential risk, continue operating with no controls, and absorb any damages that occur.
  - Rick Limitation
    - Limit the risk by implementing controls that minimize the impact of the threat.
  - Risk Transference
    - Transfer the risk by using other means to compensate for the loss, such as by purchasing insurance.

Control Evaluation

- The organization examines the costs of implementing adequate control measures against the value of those control measures.
- If the costs of implementing a control are greater than the value of the asset being protected, the control is not cost effective. I

Figure 7.2: Where Defense Mechanisms are Located.



7.5 Information Security Controls

- Physical Controls
  - prevent unauthorized individuals from gaining access to a company’s facilities.
  - Common physical controls include walls, doors, fencing, gates, locks, badges, guards, and alarm systems.
  - More sophisticated physical controls include pressure sensors, temperature sensors, and motion detectors
- Access Controls
  - restrict unauthorized individuals from using information resources and involve two major functions: authentication and authorization.
  - Authentication
    - **Something the user is:** also known as biometrics, is an authentication method that examines a person’s innate physical characteristics (e.g., fingerprint scans, palm scans, retina scans, iris recognition, and facial recognition).
    - **Something the user has:** is an authentication mechanism that includes regular identification (ID) cards, smart ID cards, and tokens.
    - **Something the user does:** is an authentication mechanism that includes voice and signature recognition.
    - **Something the user knows:** is an authentication mechanism that includes passwords and passphrases.
  - Authorization
    - the rights and privileges to which they are entitled on the organization's systems are established in a process

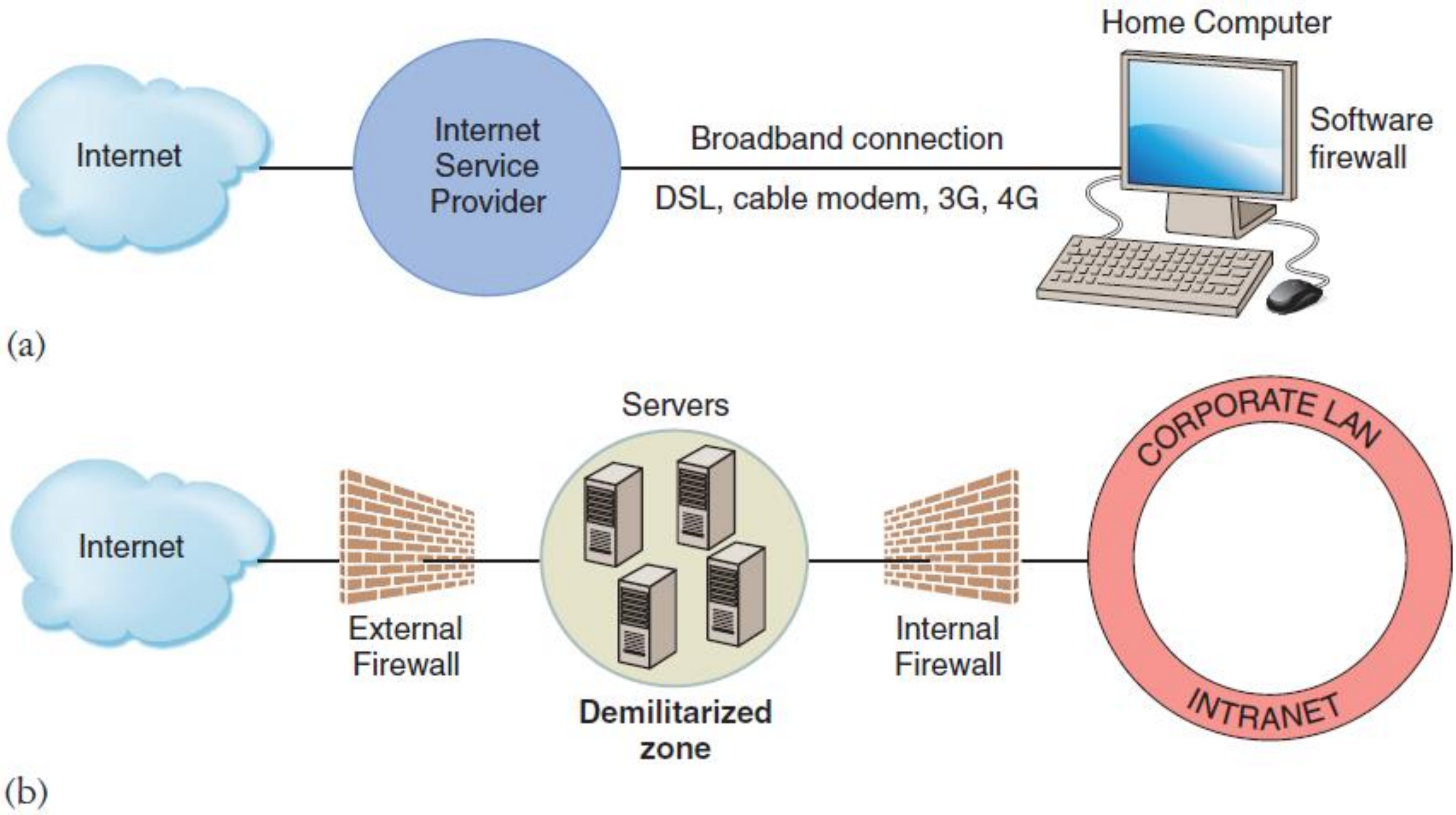
7.5 Information Security Controls

- Communications Controls(also called Network Controls)
  - secure the movement of data across networks and consist of firewalls, anti-malware systems, whitelisting and blacklisting, encryption, virtual private networks (VPNs), secure socket layer (SSL), and employee monitoring systems.
  - Communications controls consist of firewalls, anti-malware systems, whitelisting and blacklisting, encryption, virtual private networks (VPNs), transport layer security (TLS), and employee monitoring systems.

Communications Controls

- Firewall
  - a system that prevents a specific type of information from moving between untrusted networks, such as the Internet, and private networks, such as your company's network.
  - Firewalls range from simple, for home use, to very complex for organizational use.
  - Basic firewall and Corporate firewalls(Figure 7.3)
  - Demilitarized Zone (DMZ)
    - located between the two firewalls. Messages from the Internet must first pass through the external firewall.

Figure 7.3: (a) Basic Firewall for Home Computer. (b) Organization with Two Firewalls and Demilitarized Zone



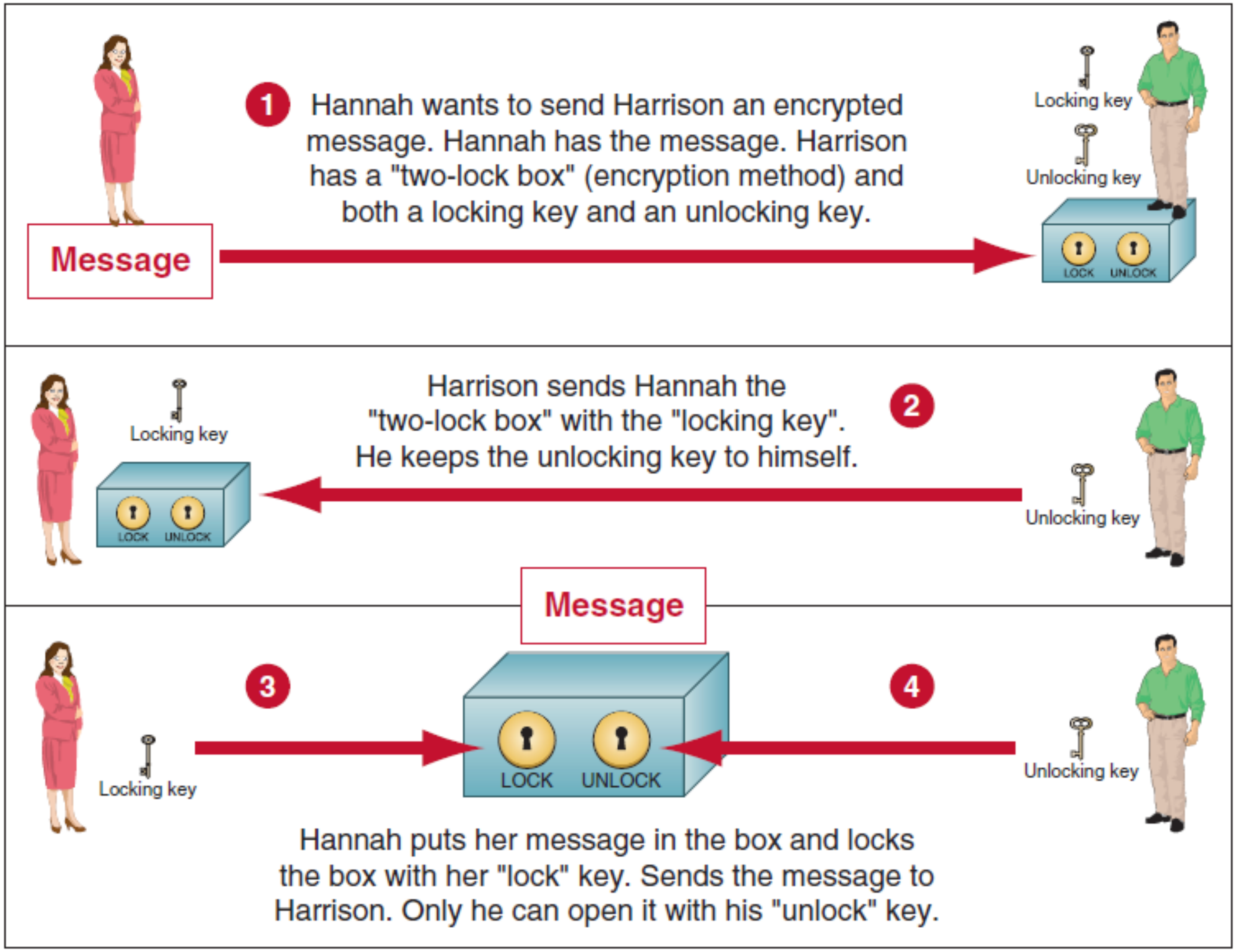
Communications Controls

- Anti-malware Systems(or antivirus software)
  - software packages that attempt to identify and eliminate viruses and worms, and other malicious software.
  - Whereas firewalls filter network traffic according to categories of activities that are likely to cause problems, anti-malware systems filter traffic according to a database of specific problems.
- Whitelisting
  - a process in which a company identifies the soft ware that it will allow to run on its computers and permits acceptable soft ware to run, and it either prevents any other soft ware from running or lets new soft ware run only in a quarantined environment until the company can verify its validity.
- Blacklisting
  - includes certain types of software that are not allowed to run in the company environment.

Communications Controls

- Encryption
  - the process of converting an original message into a form that cannot be read by anyone except the intended receiver.
  - All encryption systems use a key, which is the code that scrambles and then decodes the messages.
  - The majority of encryption systems use public-key encryption. Public-key encryption—also known as asymmetric encryption—uses two different keys: a public key and a private key
  - The public key is publicly available in a directory that all parties can access. The private key is kept secret, never shared with anyone, and never sent across the Internet. (Figure 7.4)
  - a third party, called a certificate authority, acts as a trusted intermediary between the companies. The certificate authority issues digital certificates and verifies the integrity of the certificates. A digital certificate is an electronic document attached to a file that certifies that the file is from the organization it claims to be from and has not been modified from its original format. (Figure 7.5)

Figure 7.4: How Public-key Encryption Works



1 Hannah wants to send Harrison an encrypted message. Hannah has the message. Harrison has a "two-lock box" (encryption method) and both a locking key and an unlocking key.

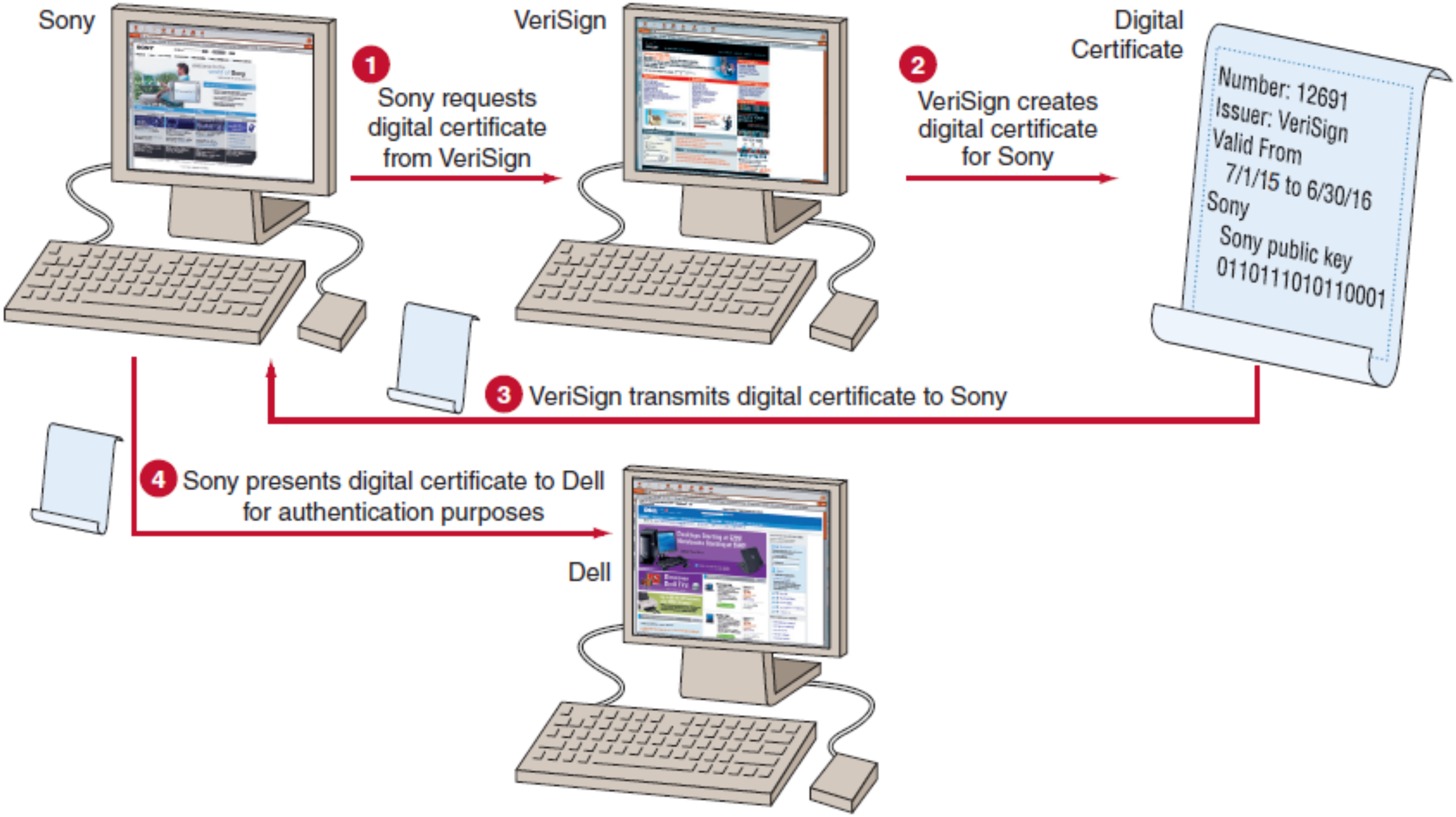
2 Harrison sends Hannah the "two-lock box" with the "locking key". He keeps the unlocking key to himself.

3

4

Hannah puts her message in the box and locks the box with her "lock" key. Sends the message to Harrison. Only he can open it with his "unlock" key.

Figure 7.5: How Digital Certificates Work.

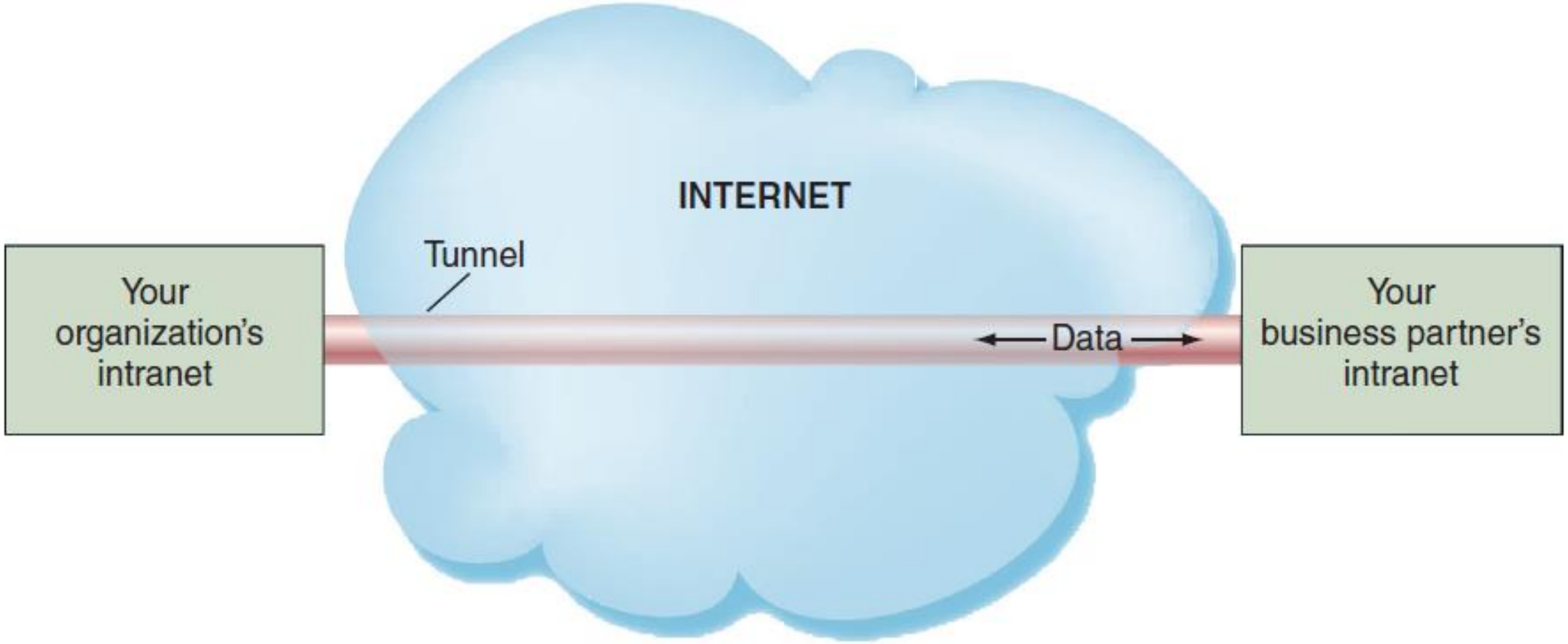


Sony
VeriSign
Digital Certificate
1 Sony requests digital certificate from VeriSign
2 VeriSign creates digital certificate for Sony
Number: 12691
Issuer: VeriSign
Valid From
7/1/15 to 6/30/16
Sony
Sony public key
0110111010110001
3 VeriSign transmits digital certificate to Sony
4 Sony presents digital certificate to Dell for authentication purposes
Dell

Communications Controls

- Virtual Private Network (VPN)
  - a private network that uses a public network (usually the Internet) to connect users. VPNs essentially integrate the global connectivity of the Internet with the security of a private network and thereby extend the reach of the organization’s networks. VPNs are called virtual because they have no separate physical existence.

Figure 7.6: Virtual Private Network (VPN) and Tunneling


INTERNET
Tunnel
Your organization's intranet
Data
Your business partner's intranet

Communications Controls (Continued)

- Transport Layer Security (formerly called Secure Socket Layer)
  - formerly called secure socket layer, is an encryption standard used for secure transactions such as credit card purchases and online banking. TLS encrypts and decrypts data between a Web server and a browser end to end.
- Employee Monitoring Systems
  - scrutinize their employees’ computers, e-mail activities, and Internet surfing activities. These products are useful to identify employees who spend too much time surfing on the Internet for personal reasons, who visit questionable Web sites, or who download music illegally.

Business Continuity Planning

- Business Continuity
  - the chain of events linking planning to protection and to recovery.
- Business Continuity Plan
  - purpose is to provide guidance to people who keep the business operating aft er a disaster occurs.

Information Systems Auditing

- **Audit:**
  - an examination of information systems, their inputs, outputs, and processing.
- Internal Audits
- External Audits
- IS auditing focuses on issues such as operations, data integrity, software applications, security and privacy, budgets and expenditures, cost control, and productivity.
- Guidelines are available to assist auditors in their jobs, such as those from the Information Systems Audit and Control Association (www.isaca.org).

Three Categories of IS auditing procedures:

- Auditing Around the Computer
  - means verifying processing by checking for known outputs using specific inputs. This approach is most effective for systems with limited outputs.
- Auditing Through the Computer
  - auditors check inputs, outputs, and processing. They review program logic, and they test the data contained within the system.
- Auditing With the Computer
  - means using a combination of client data, auditor soft ware, and client and auditor hardware. This approach enables the auditor to perform tasks such as simulating payroll program logic using live data.