CHAPTER 7

Information Security

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

1. Identify the five factors that contribute to the increasing vulnerability of information resources, and provide a specific example of each one.
2. Compare and contrast human mistakes and social engineering, and provide a specific example of each one.
3. Discuss the 10 types of deliberate attacks.

4. Define the three risk mitigation strategies, and provide an example 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, and provide an example of each one.

OPENING >

- **Shodan: Good Tool or Bad Tool?**
  1. Is Shodan more useful for hackers or for security defenders? Provide specific examples to support your choice.
  2. What impact should Shodan have on the manufacturers of devices that connect to the Internet?
  3. As an increasingly large number of devices are connected to the Internet, what will Shodan’s impact be? Provide examples to support your answer.

7.1 Introduction to Information Security

- Information Security
- Threat
- Exposure
- Vulnerability
- Five Key Factors Increasing Vulnerability
- Cybercrime

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

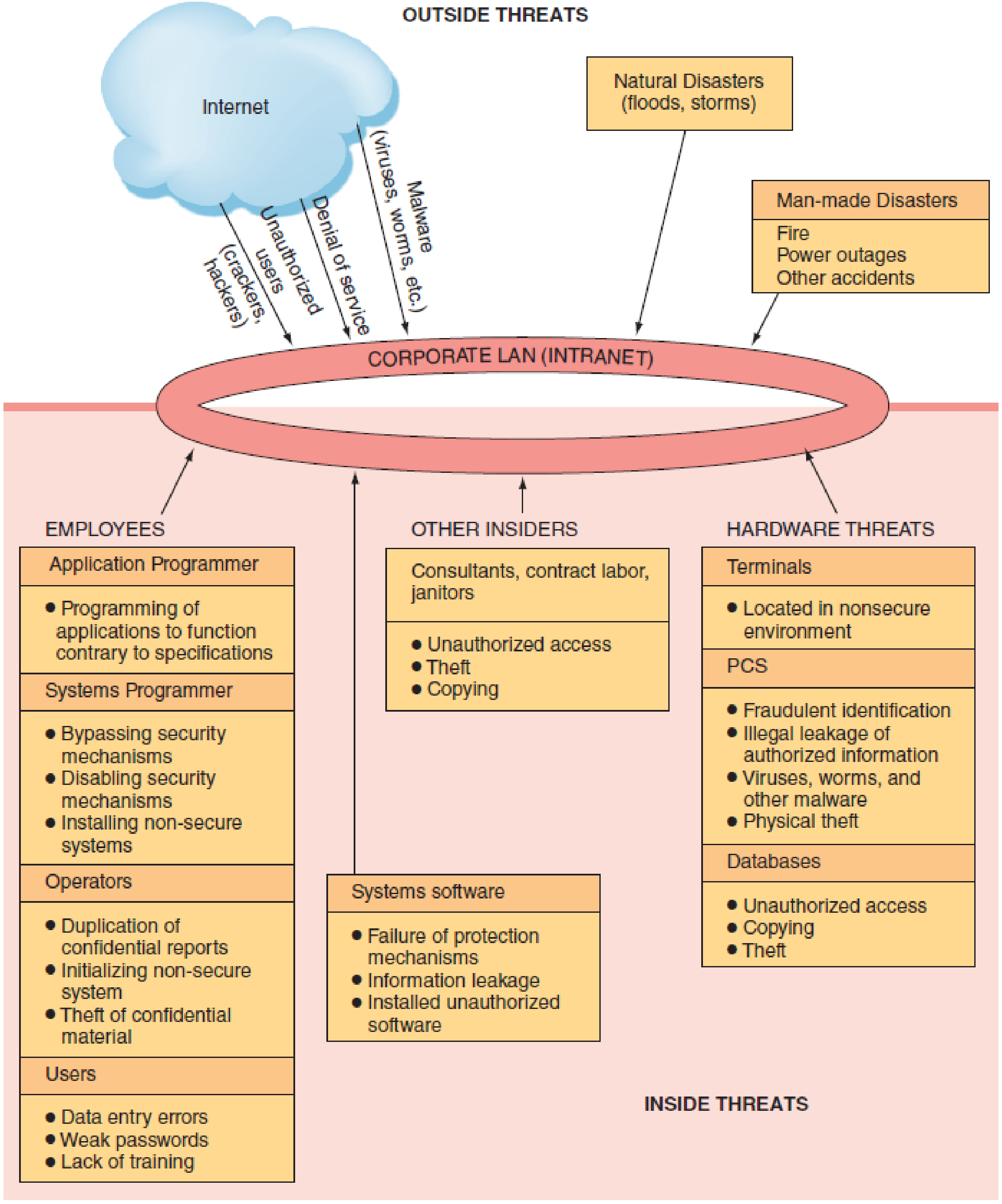
Human Errors

- Higher employee levels = higher levels of security risk
- Most Dangerous Employees
- Human Mistakes

Dangerous Employees

- Two organizational areas pose the greatest risk
  - Human Resources
  - Information Systems
- Janitors and Guards Frequently Overlooked

Figure 7.1 Security Threats:



Natural Disasters (floods, storms)

Man-made Disasters
- Fire
- Power outages
- Other accidents

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

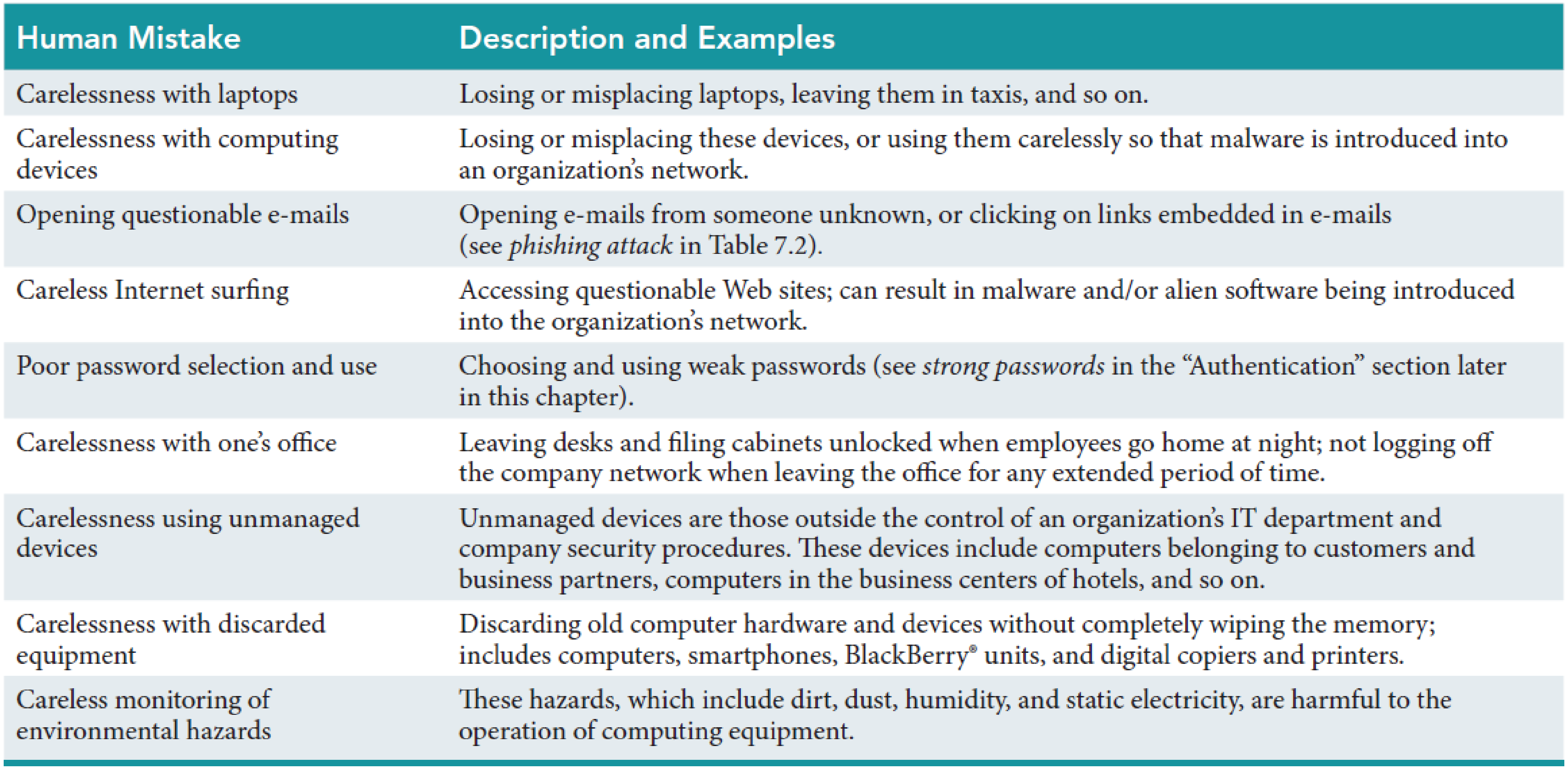
Human Mistakes

- Carelessness with laptops
- Carelessness with computing devices
- Opening questionable e-mails
- Careless Internet surfing
- Poor password selection and use
- Carelessness with one’s office

Human Mistakes (continued)

- Carelessness using unmanaged devices
- Carelessness with discarded equipment
- Careless monitoring of environmental hazards

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

Blend/Image Source Limited

Who is real and who is engaged in social engineering? Can you tell?

- **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.

7.3 Deliberate Threats to Information Systems

1. Espionage or Trespass
2. Information Extortion
3. Sabotage or Vandalism
4. Theft of Equipment or Information
5. Identity Theft
6. Compromises to Intellectual Property

7.3 Deliberate Threats to Information Systems (continued)

7. Software Attacks
8. Alien Software
9. Supervisory Control and Data Acquisition Attacks
10. Cyberterrorism and Cyberwarfare

Compromises to Intellectual Property

- Intellectual Property
- Trade Secret
- Patent
- Copyright

Software Attacks: Three Categories

1. Remote Attacks Requiring User Action
   - Virus
   - Worm
   - Phishing Attack
   - Spear Phishing

Software Attacks: Three Categories (continued)

2. Remote Attacks Needing No User Action
   - Denial-of-Service Attack
   - Distributed Denial-of-Service Attack

Software Attacks: Three Categories (continued)

3. Attacks by a Programmer Developing a System
   - Trojan Horse
   - Back Door
   - Logic bomb

IT'S ABOUT BUSINESS 7.1

- **Stealing Cash from ATMs with Text Messages**

  1. Other than the ones mentioned in this case, what countermeasures could banks take to defend against ATM hacks such as these?
  2. Why are some banks still using Windows XP on their ATMs, when newer, more secure operating systems are available?

Alien Software

- Adware
- Spyware
- Spamware
- Spam
- Cookies

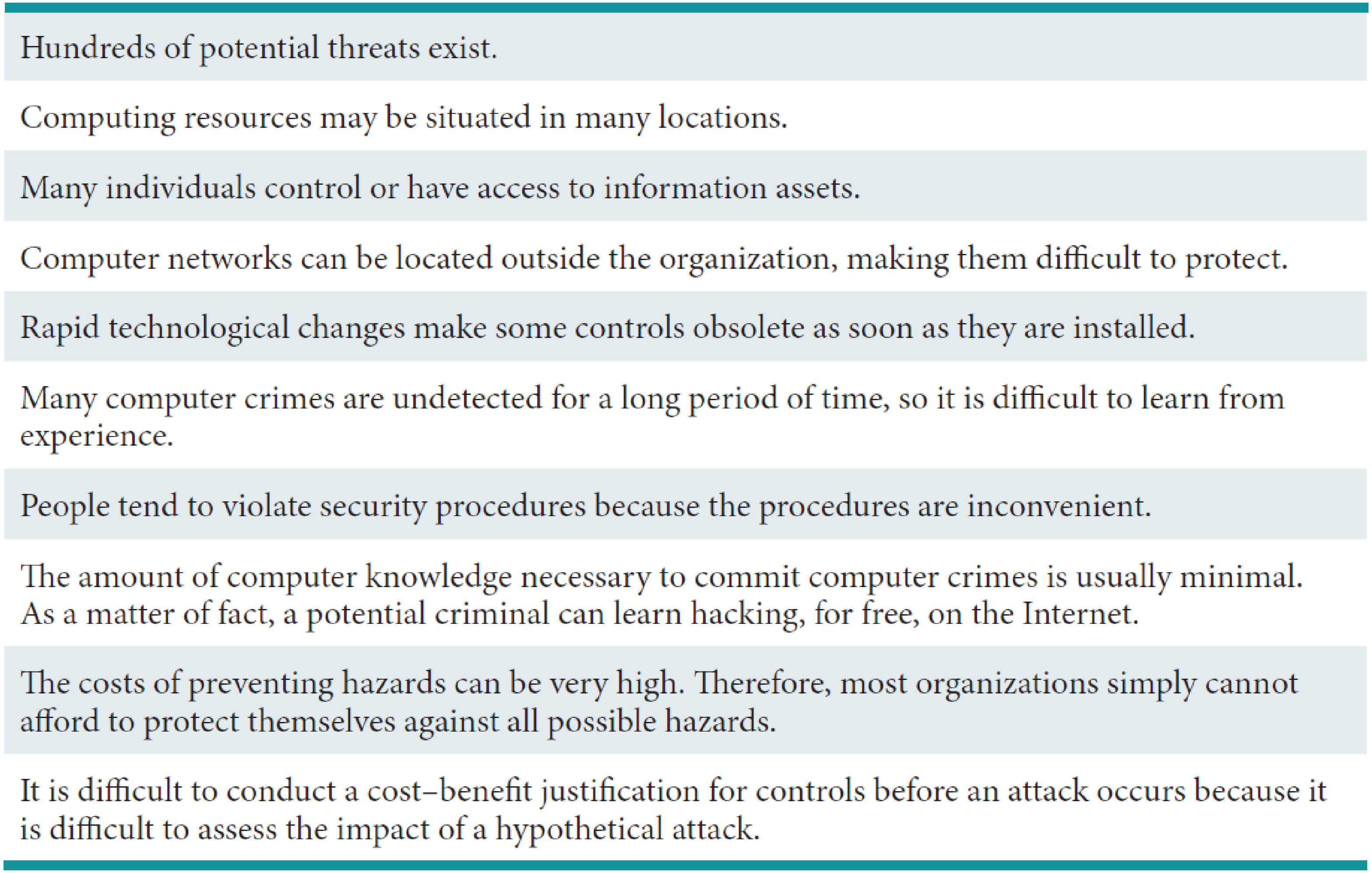
IT'S ABOUT BUSINESS 7.2

- **The Mask**
  1. Discuss the implications of the targeted nature of the Careto malware.
  2. Analyze the statement: "Nations use malware such as Careto when their only alternative is to go to war."
  3. Discuss the impacts that such sophisticated malware could have on all of us.

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

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

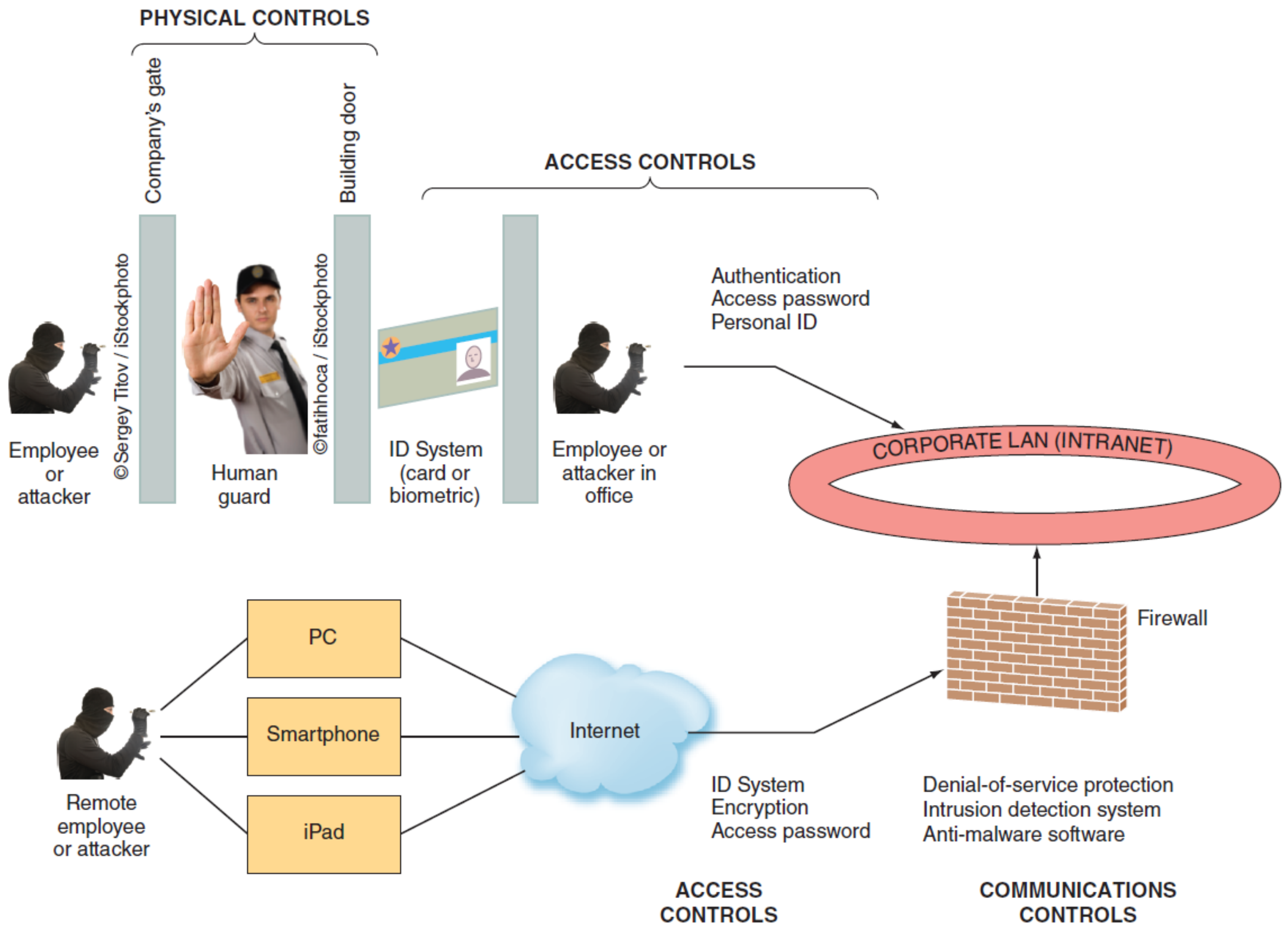
Risk Mitigation

- Risk Acceptance
- Rick Limitation
- Risk Transference

7.5 Information Security Controls

- Physical Controls
- Access Controls
- Communications Controls
- Business Continuity Planning
- Information Systems Auditing

Figure 7.2: Where Defense Mechanisms are Located.



Physical Controls

- Walls
- Doors
- Fencing
- Gates
- Locks
- Badges
- Guards
- Alarm Systems

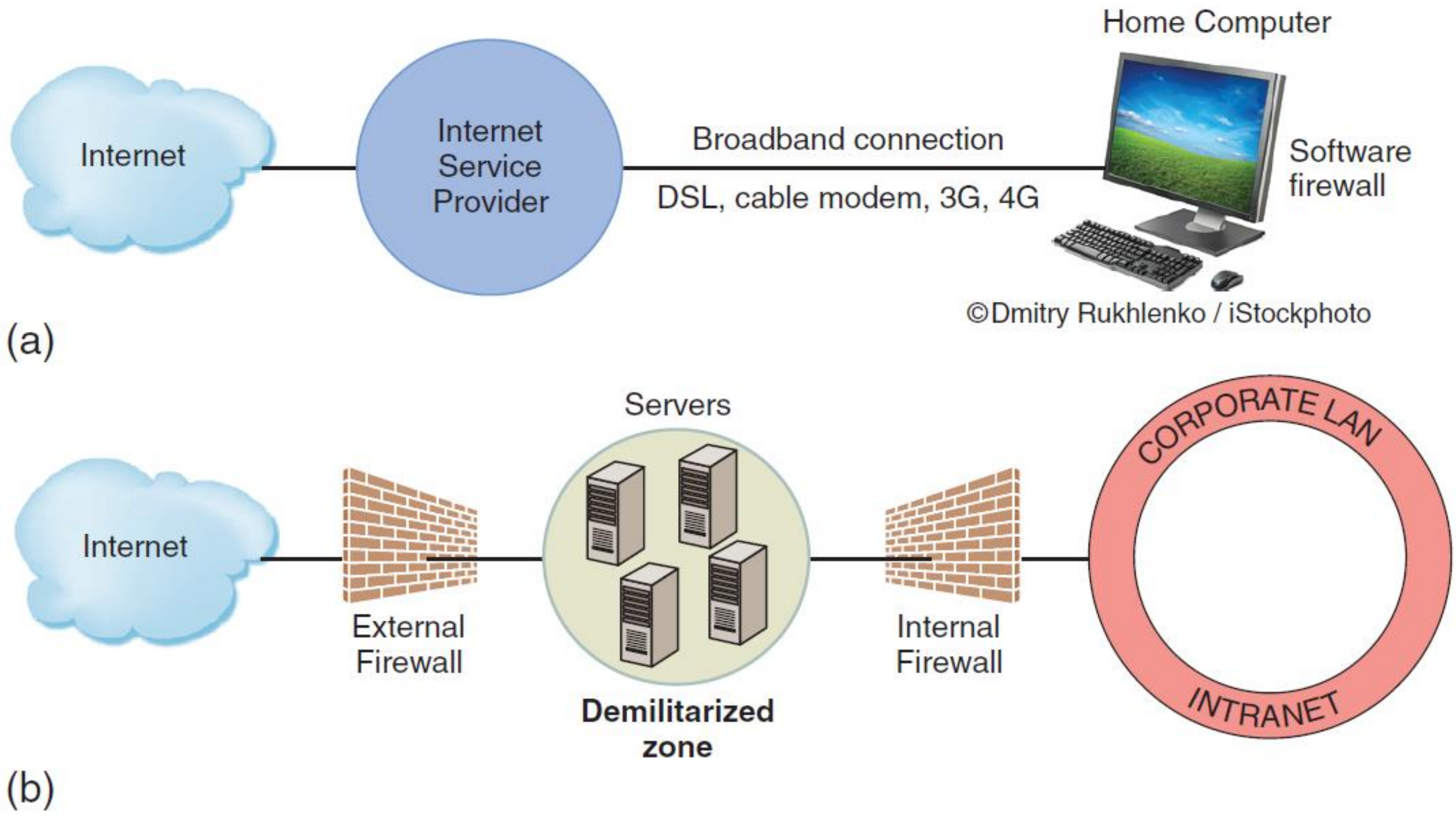
Access Controls

- Authentication
- Authorization
  - Something the user is
  - Something the user has
  - Something the user does
  - Something the user knows

Communications Controls

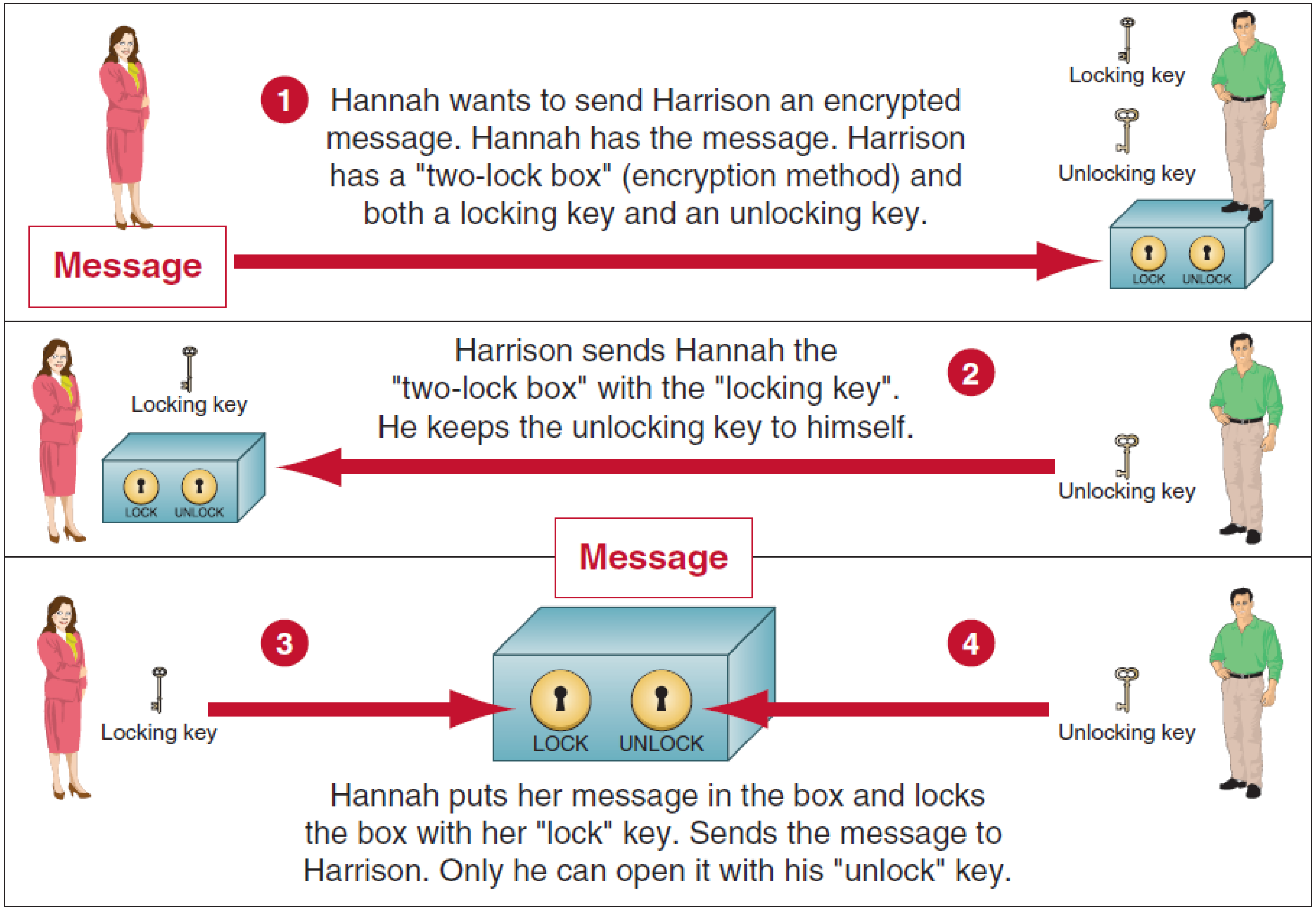
- Firewall
- Anti-malware Systems
- Whitelisting
- Blacklisting
- Encryption
- Virtual Private Network (VPN)

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



©Dmitry Rukhlenko / iStockphoto

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.

Courtesy of Brad Prince.

Figure 7.5: How Digital Certificates Work.

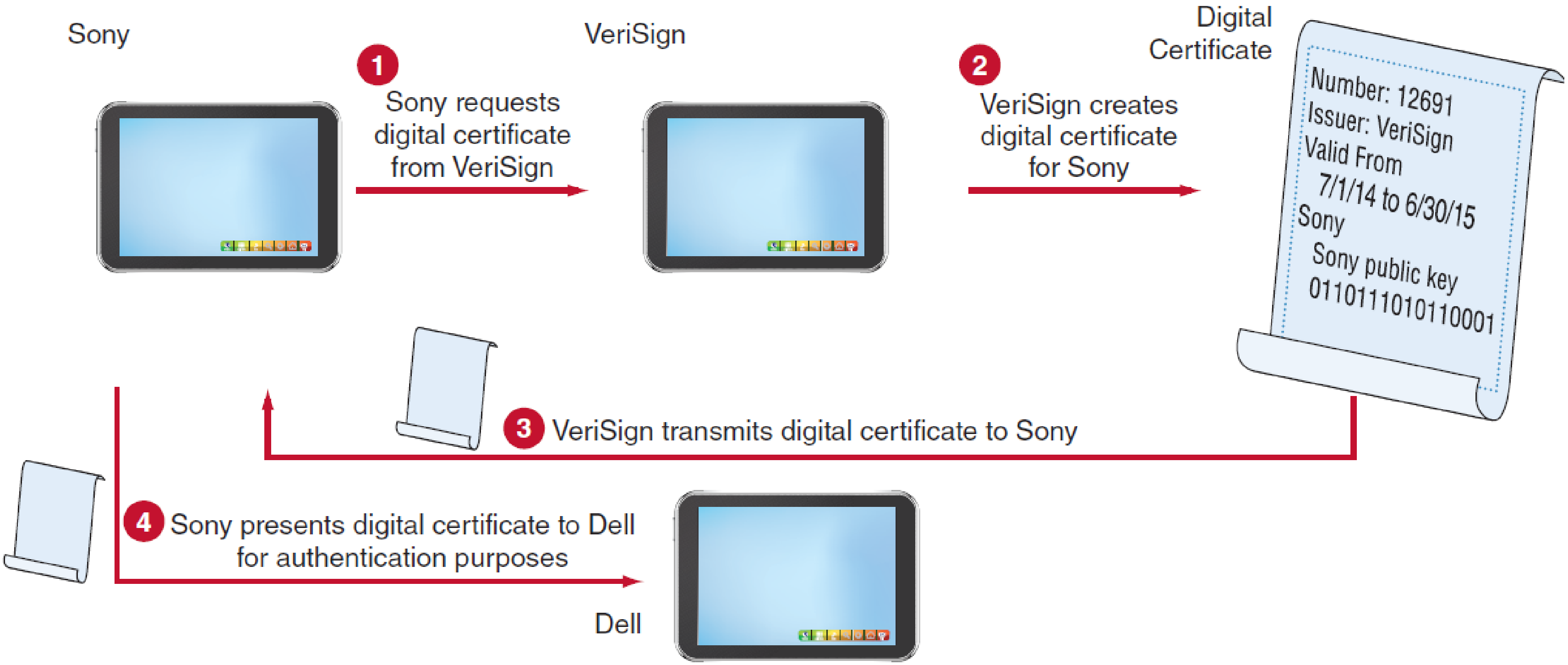
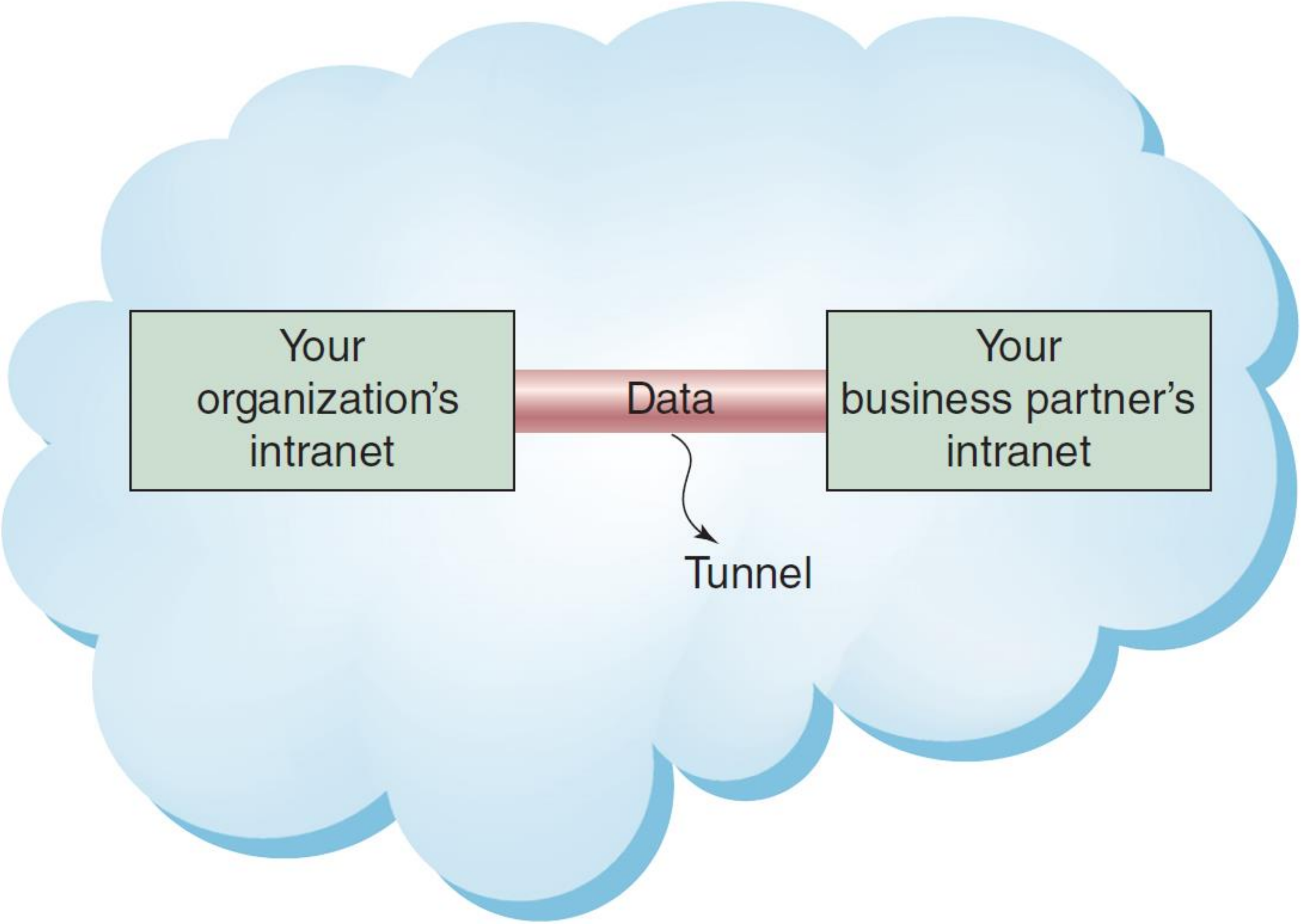

Sony
VeriSign
Digital Certificate
1 Sony requests digital certificate from VeriSign
2 VeriSign creates digital certificate for Sony
Number: 12691
Issuer: VeriSign
Valid From
7/1/14 to 6/30/15
Sony
Sony public key
0110111010110001
3 VeriSign transmits digital certificate to Sony
4 Sony presents digital certificate to Dell for authentication purposes
Dell

Figure 7.6: Virtual Private Network (VPN) and Tunneling


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

IT'S ABOUT BUSINESS 7.3

- **A Tale of Two Cybersecurity Firms**
  1. Describe why it was so important for law enforcement officials to capture all 96 Rustock command servers at one time.
  2. If the perpetrators of Rustock are ever caught, will it be possible to prove that they were responsible for the malware? Why or why not? Support your answer.
  3. Mandiant has stated that it has no definitive proof that Chinese hackers are behind the numerous attacks on U.S. companies and government agencies. Is such proof even possible to obtain? Why or why not? Support your answer. If such proof were possible to obtain, would it matter? Why or why not? Support your answer.
  4. Discuss the advantages for FireEye of purchasing Mandiant. Then, discuss the benefits that Mandiant obtained from the sale.

Business Continuity Planning

- Business Continuity
- Business Continuity Plan

Information Systems Auditing

- Internal Audits
- External Audits
- Three Categories of IS auditing procedures

Three Categories of IS auditing procedures:

- Auditing Around the Computer
- Auditing Through the Computer
- Auditing With the Computer