Chapter 2

The Modern Organization in the Digital Economy

Learning Objectives

- Describe the characteristics of the digital economy and e-business.
- Discuss the relationships among business pressures, organizational responses and information systems.
- Describe strategic information systems (SISs) and explain their advantages.

Learning Objectives (Continued)

- Describe Porter's competitive force model and how information technology helps companies improve their competitive positions.
- Describe five strategies that companies can use to achieve competitive advantage in their industries.

2.1 Doing Business in the Digital Economy

- The **digital economy** is an economy based on digital technologies, including communication networks (the Internet, intranets, and extranets), computers, software, and other related technologies.
- Also called the *Internet economy*, the *new economy*, or the *Web economy* .
- Digital infrastructures provide a **global platform** over which people and organizations interact, communicate, collaborate, and search for information.

The Global Platform of the New Economy

- A huge number of digitizable products; that is products that can be converted to digital format. Most common are: books, movies, magazines, TV and radio programming, electronic games, music CDs and computer software.
- Consumers and firm conducting financial transaction digitally.
- Physical goods such as home appliances and automobiles that contain embedded computer chips and connectivity capabilities.

Electronic Business

- Businesses increasingly perform their basic functions: buying and selling goods and services, servicing customers, and collaborating with business partners electronically.
- This process is known as **electronic business (E-business)** or **electronic commerce (E-commerce).**

New Economy vs. Old Economy

Example	Old	New
Buying and selling text book	Visit the bookstore	Visit web site for publishers and retailers
Registering for classes	Walk around campus to Departments, Registrar's office, etc.	Access campus web site
Photography	Buy film, use camera, take picture, take it for processing	Use digital camera
Paying for Gasoline	Fill up your car, go inside, pay cash or credit card	Use speed pass token wave over the sensor and go
Paying the Transportation	Pay cash, metal tokens	Metro cards electronic cards
Paying for goods	Visit store, take the item, pay , go	Use self – service kiosks
Supplying commercial photos	Use newspapers, paper, catalog or on line	Use hub-like supply chain with digitized picture

2.2 Business Pressures, Organizational Responses, and IT Support

- **Business Pressure -** The business environment is the combination of social, legal, economic, physical, and political factors that affect business activities.
- Significant changes in any of these factor are likely to create business pressure on the organization.
- The three types of business pressures faced are: *market*, *technology*, and *societal pressures*.

IT Support for Organizational Responses to Business Pressures

Three Types of Business Pressures

- **Market Pressures**:
  - The Global Economy and Strong Competition
  - The Changing Nature of the Workforce
  - Powerful Customers

Business Pressures (Continued)

- **Technology Pressures**:
  - Technological Innovation and Obsolescence
  - Information Overload

Business Pressures (Continued)

- **Societal Pressures**:
  - Social Responsibility
  - Government Regulation and Deregulation
  - Protection Against Terrorist Attacks.
  - Ethical Issues

Organizational Responses

- **Strategic Systems** provide advantages that enable organizations to increase market share and/or profits, to better negotiate with suppliers, or prevent competitors from entering their markets.
- **Customer Focus** is the difference between attracting and keeping customers by providing superb customer service to losing them to competitors.

Organizational Responses (Continued)

- **Make-to-Order** is a strategy of producing customized products and services.
- **Mass Customization** is producing a large quantity of items, but customizing them to fit the desire of each customer.
- **E-business** and **E-commerce** is the strategy of doing business electronically.

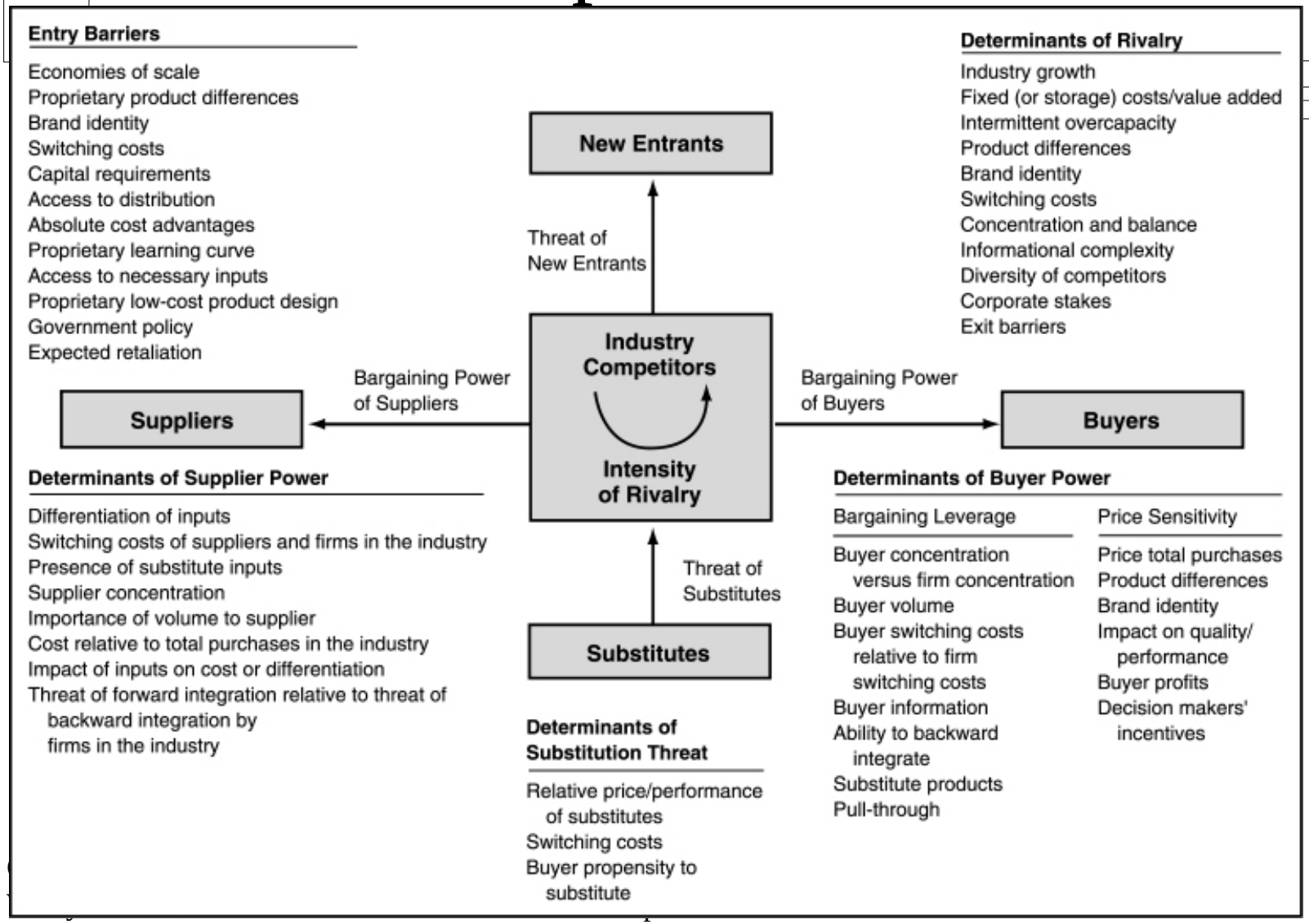
2.3 Competitive Advantage and Strategic Information Systems

- **Competitive Advantage**: An advantage over competitors in some measure such as cost, quality, or speed, leads to control of a market and to larger-than average profits.
- **Strategic Information Systems** (**SIS**) provide a competitive advantage by helping an organization to implement its strategic goals and to increase its performance and productivity.

Porter's Competitive Forces Model

- The best-known framework for analyzing competitiveness is Michael Porter's **competitive forces model** (Porter, 1985).
- Model is used to develop strategies to increase their competitive edge.
- Demonstrates how IT can make a company more competitive.

Porter's Competitive Forces Model



Competitive Forces

- If a business wants to succeed must develop strategies to counter these forces:
  - Rivalry of competitors within its industry
  - Threat of new entrants into an industry and its markets
  - Threat posed by substitute products which might capture market share
  - Bargaining power of customers
  - Bargaining power of suppliers

5 forces and Internet

1. The threat of entry of new competitor
   - The Internet increases the threat that new competitors will enter the market. (no sales force or physical storefront to sell goods).
2. The bargaining power of supplier
   - Buyer can find alternative suppliers and compare prices more easily.
3. The bargaining power of customer (buyers)
   - Greatly increases customer's access to information about product and suppliers.

5 forces and Internet (cont'd)

4. The threat of substitute product or services
   - Information-based industries are in the greatest danger from substitutes. Any industries in which digitized information can replace material goods (e.g., music, books, software)
5. The rivalry among existing firms in the industry
   - The visibility of Internet applications on the web makes proprietary systems more difficult to keep secret.

Five Competitive Strategies

- Cost Leadership
  - Become low-cost producers
  - Help suppliers or customers reduce costs
  - Increase cost to competitors
  - Example, Walmart's automatic inventory replenishment system.
- Differentiation Strategy
  - Develop ways to differentiate a firm's products from its competitors
  - Can focus on particular segment or niche of market
  - Example, AusPost uses tracking systems.

Competitive Strategies *(cont.)*

- Innovation Strategy
  - Find new ways of doing business
    - Unique products or services
    - Or unique markets
    - Radical changes to business processes to alter the fundamental structure of an industry
  - Example, Amazon uses online full-service customer systems
- Operational effectivenes Strategy
  - Improve the manner of internal business process.
  - Lead to improvement in quality, productivity, employee and customer satisfaction.
  - Example, improvement in Toronto 1 of Toronto's International Airport which saved both the airport and the airlines money.

Competitive strategies *(cont.)*

- Alliance Strategy
  - Establish linkages and alliances with
    - Customers, suppliers, competitors, consultants and other companies
  - Includes mergers, acquisitions, joint ventures, virtual companies
  - Example, Wal-Mart uses automatic inventory replenishment by supplier

Using these strategies

- The strategies are not mutually exclusive
- Organizations use one, some or all

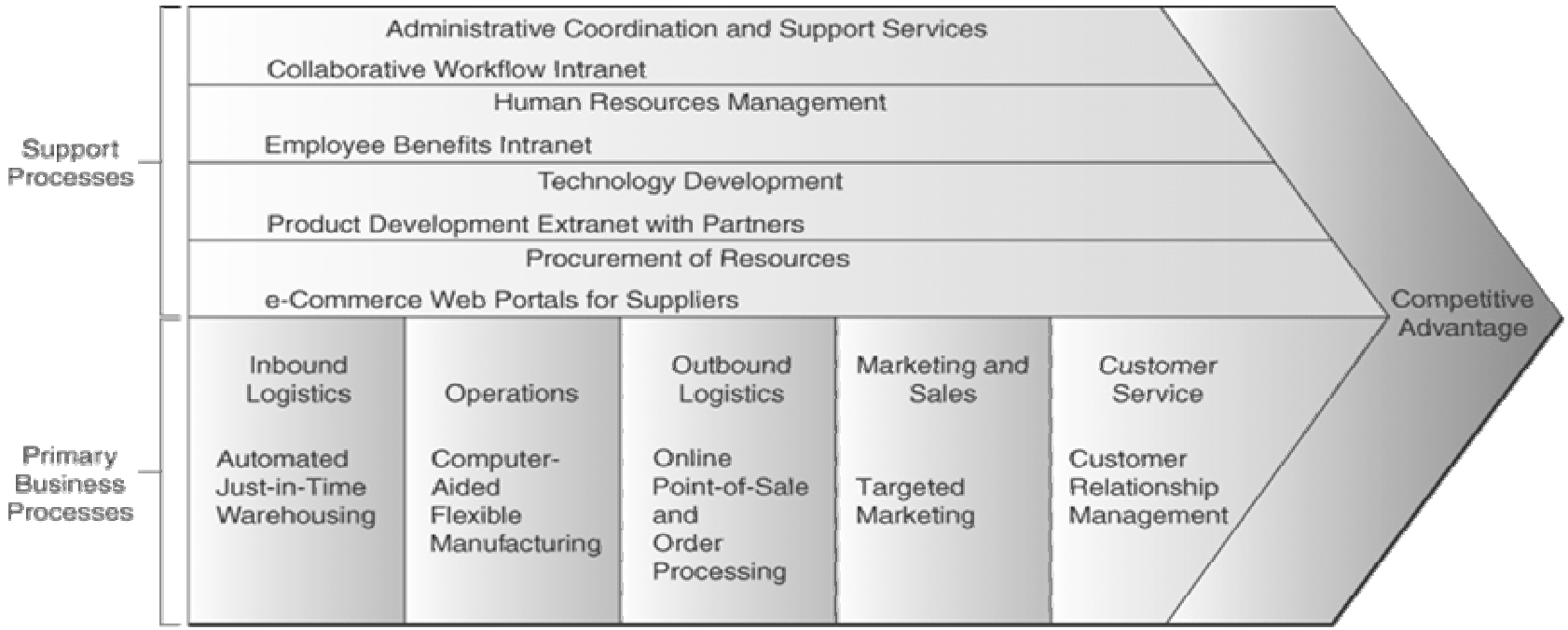
Using IT for these strategies

Basic Strategies in the Business Use of Information Technology
Lower Costs • Use IT to substantially reduce the cost of business processes. • Use IT to lower the costs of customers or suppliers.
Differentiate • Develop new IT features to differentiate products and services. • Use IT features to reduce the differentiation advantages of competitors. • Use IT features to focus products and services at selected market niches.
Innovate • Create new products and services that include IT components. • Develop unique new markets or market niches with the help of IT. • Make radical changes to business processes with IT that dramatically cut costs, improve quality, efficiency, or customer service, or shorten time to market.
Promote Growth • Use IT to manage regional and global business expansion. • Use IT to diversify and integrate into other products and services.
Develop Alliances • Use IT to create virtual organizations of business partners. • Develop interenterprise information systems linked by the Internet and extranets that support strategic business relationships with customers, suppliers, subcontractors, and others.

Value Chain

- View the firm as a chain of basic activities that add value to its products and services
- Activities are either
  - Primary processes directly related to manufacturing or delivering products
  - Support processes help support the day-to-day running of the firm and indirectly contribute to products or services
- Use the value chain to highlight where competitive strategies can best be applied to add the most value

Using IS in the value chain



Chapter 3

Ethics, Privacy and Information Security

Learning Objectives

- Describe the major ethical issues related to information technology and identify situations in which they occur.
- Describe the many threats to information security.
- Understand the various defense mechanisms used to protect information systems.
- Explain IT auditing and planning for disaster recovery.

3.1 Ethical Issues

- **Ethics**. A branch of philosophy that deals with what is considered to be right and wrong.
- A **Code of Ethics** is a collection of principles that are intended to guide decision making by members of an organization.

The Four Categories of Ethical Issues

- ***Privacy Issues*** involves collecting, storing and disseminating information about individuals.
- ***Accuracy Issues*** involves the authenticity, fidelity and accuracy of information that is collected and processed.
- ***Property Issues*** involves the ownership and value of information.
- ***Accessibility Issues*** revolve around who should have access to information and whether they should have to pay for this access.

Protecting Privacy

- **Privacy**. The right to be left alone and to be free of unreasonable personal intrusions.
- Two rules have been followed fairly closely in past court decision in many countries:
  - *The right of privacy is not absolutes*. Privacy must be balanced against the needs of society
  - The public's right to know is superior to the individual's right of privacy.

Protecting Privacy (Continued)

- **Electronic Surveillance**. The tracking of people‘s activities, online or offline, with the aid of computers.
- **Personal Information in Databases**. Information about individuals is being kept in many databases: banks, utilities co., govt. agencies, …etc.; the most visible locations are credit-reporting agencies.

Protecting Privacy (Continued)

- **Information on Internet Bulletin Boards and Newsgroups**. *Electronic discussions* such as **chat rooms** and these other sites appear on the Internet, within corporate intranets, and on **blogs**.
- A *blog* (Weblog) is an informal, personal journal that is frequently updated and intended for general public reading.

Protecting Privacy (Continued)

- **Privacy Codes and Policies.** An organization's guidelines with respect to protecting the privacy of customers, clients, and employees.
- **International Aspects of Privacy**. Privacy issues that international organizations and governments face when information spans countries and jurisdictions.

3.2 Threats to Information Security

- A **threat** to an information resource is any danger to which a system may be exposed.
- The **exposure** of an information resources is the harm, loss or damage that can result if a threat compromises that resource.
- A system's **vulnerability** is the possibility that the system will suffer harm by a threat.
- **Risk** is the likelihood that a threat will occur.
- **Information system controls** are the procedures, devices, or software aimed at preventing a compromise to the system.

Unintentional Threats

- *Human errors* can occur in the design of the hardware and/or information system.
- Also can occur in programming, testing, data collection, data entry, authorization and procedures.
- Contribute to more than 50% of control and security-related problems in organizations.

Unintentional Threats (Continued)

- *Environmental hazards* include earthquakes, severe storms, floods, power failures or strong fluctuations, fires (most common hazard), explosions, …etc.
- *Computer system failures* can occur as the result of poor manufacturing or defective materials.

Intentional Threats

- Typically, criminal in nature.
- **Cybercrimes** are fraudulent activities committed using computers and communications networks, particularly the Internet.
- Average cybercrime involves about $600,000 according to FBI.

Intentional Threats (Continued)

- **Hacker.** An outside person who has penetrated a computer system, usually with no criminal intent.
- **Cracker.** A malicious hacker.
- **Social engineering.** Computer criminals or corporate spies get around security systems by building an inappropriate trust relationship with insiders.

Espionage or Trespass

- The act of gaining access to the information an organization is trying to protect by an unauthorized individual.
- *Industrial espionage* occurs in areas where researching information about the competition goes beyond the legal limits.
- Governments practice *industrial espionage* against companies in other countries.
- *Shoulder surfing* is looking at a computer monitor or ATM screen over another person's shoulder.

Sabotage or Vandalism

- A popular type of online vandalism is ***hacktivist*** or ***cyberactivist*** activities.
- ***Hacktivist*** or ***cyberactivist*** use technology for high-tech civil disobedience to protest operations, policies, or actions of an individual, an organization, or a government agency.

Sabotage or Vandalism (Continued)

- **Cyberterrorism** is a premeditated, politically motivated attack against information, computer systems, computer programs, and data that results in violence against noncombatant targets by subnational groups or clandestine agents.
- **Cyberwar**. War in which a country's information systems could be paralyzed from a massive attack by destructive software.
- **Theft** is the illegal taking of property that belongs to another individual or organization.

Identity Theft

- Crime in which someone uses the personal information of others, usually obtained from the Internet, to create a false identity and then commits fraud.
- Fastest growing white-collar crime.
- Biggest problem is restoring victim's damaged credit rating.

Software Attacks

- ***Malicious software (malware)*** designed to damage, destroy, or deny service to the targeted systems.
- Most common types of software attacks are viruses, worms, Trojan horses, logic bombs, back doors, denial-of-service, alien software, phishing and pharming.

Software Attacks (Continued)

- **Viruses.** Segments of computer code that performs unintended actions ranging from merely annoying to destructive.
- **Worms.** Destructive programs that replicate themselves without requiring another program to provide a safe environment for replication.
- **Trojan horses.** Software programs that hide in other computer programs and reveal their designed behavior only when they are activated.

Software Attacks (Continued)

- **Logic bombs.** Designed to activate and perform a destructive action at a certain time.
- **Back doors or trap doors.** Typically a password, known only to the attacker, that allows access to the system without having to go through any security.
- **Denial-of-service.** An attacker sends so many information requests to a target system that the target cannot handle them successfully and can crash the entire system.

Alien Software

- **Pestware.** Clandestine software that uses up valuable system resources and can report on your Web surfing habits and other personal information.
- **Adware.** Designed to help popup advertisements appear on your screen.
- **Spyware.** Software that gathers user information through the user's Internet connection without their knowledge (i.e. keylogger, password capture).

Alien Software (Continued)

- **Spamware.** Designed to use your computer as a launch pad for spammers.
- **Spam.** Unsolicited e-mail, usually for purposes of advertising.
- **Cookies.** Small amount of information that Web sites store on your computer, temporarily or more-or-less permanently.

Alien Software (Continued)

- **Web bugs.** Small, usually invisible, graphic images that are added to a Web page or e-mail.
- **Phishing.** Uses deception to fraudulently acquire sensitive personal information such as account numbers and passwords disguised as an official-looking e-mail.
- **Pharming.** Fraudulently acquires the Domain Name for a company's Web site and when people type in the Web site url they are redirected to a fake Web site.

Compromises to Intellectual Property

- **Intellectual property**. Property created by individuals or corporations which is protected under *trade secret*, *patent*, and *copyright* laws.
- **Trade secret.** Intellectual work, such as a business plan, that is a company secret and is not based on public information.
- **Patent.** Document that grants the holder exclusive rights on an invention or process for 20 years.

Compromises to Intellectual Property (Continued)

- **Copyright.** Statutory grant that provides creators of intellectual property with ownership of the property for life of the creator plus 70 years.
- **Piracy.** Copying a software program without making payment to the owner.

3.3 Protecting Information Resources

- **Risk.** The probability that a threat will impact an information resource.
- **Risk management.** To identify, control and minimize the impact of threats.
- **Risk analysis.** To assess the value of each asset being protected, estimate the probability it might be compromised, and compare the probable costs of it being compromised with the cost of protecting it.

Protecting Information Resources (Continued)

- **Risk mitigation** is when the organization takes concrete actions against risk. It has two functions:
  - (1) implement controls to prevent identified threats from occurring, and
  - (2) developing a means of recovery should the threat become a reality.

Risk Mitigation Strategies

- **Risk Acceptance.** Accept the potential risk, continue operating with no controls, and absorb any damages that occur.
- **Risk limitation.** Limit the risk by implementing controls that minimize the impact of threat.
- **Risk transference.** Transfer the risk by using other means to compensate for the loss, such as purchasing insurance.

Controls

- **Controls evaluation.** Identifies security deficiencies and calculates the costs of implementing adequate control measures.
- **General controls.** Established to protect the system regardless of their application.
  - **Physical controls.** Physical protection of computer facilities and resources.
  - **Access controls.** Restriction of unauthorized user access to computer resources; use **biometrics** and **passwords** controls for user identification.

Controls (Continued)

- **Communications (networks) controls.** To protect the movement of data across networks and include border security controls, authentication and authorization.
  - **Firewalls.** System that enforces access-control policy between two networks.
  - **Encryption.** Process of converting an original message into a form that cannot be read by anyone except the intended receiver.

Controls (Continued)

- All **encryption** systems use a key.
- **Symmetric encryption.** Sender and the recipient use the same key.
- **Public-key encryption.** Uses two different keys: a public key and a private key.
- **Certificate authority.** Asserts that each computer is identified accurately and provides the public keys to each computer.

Controls (Continued)

- **Virtual Private Networking.** Uses the Internet to carry information within a company and among business partners but with increased security by uses of encryption, authentication and access control.
- **Application controls.** Controls that protect specific applications and include: input, processing and output controls.

Controls (Continued)

- **Information systems auditing.** Independent or unbiased observers task to ensure that information systems work properly.
- **Types of Auditors and Audits**
  - **Internal.** Performed by corporate internal auditors.
  - **External.** Reviews internal audit as well as the inputs, processing and outputs of information systems.
  - **Audit.** Examination of information systems, their inputs, outputs and processing.

Disaster Recovery Planning

- **Disaster recovery.** The chain of events linking planning to protection to recovery, *disaster recovery plan*.
- **Disaster avoidance.** Oriented towards prevention, *uninterrupted power supply (UPS)*.
- **Hot sites.** External data center that is fully configured and has copies of the organization's data and programs.

- Thanks.