Chapter 16

Managing Information Resources and Security

Information Technology For Management 6th Edition
Turban, Leidner, McLean, Wetherbe
Lecture Slides by L. Beaubien, Providence College

John Wiley & Sons, Inc.

Learning Objectives

- Recognize the business value of security and control
- Understand the role of the IS department and its relationships with end users.
- Discuss the role of the chief privacy officer.
- Recognize information systems’ vulnerability, threats, attack methods, and the possible symptoms of attack.

Learning Objectives (Continued)

- Describe the major methods of defending information systems.
- Describe internal control and fraud.
- Describe the security issues of the Web and electronic commerce.
- Describe business continuity and disaster recovery planning.
- Understand the role of computer forensics in investigating and deterring security.

Security & the Enterprise

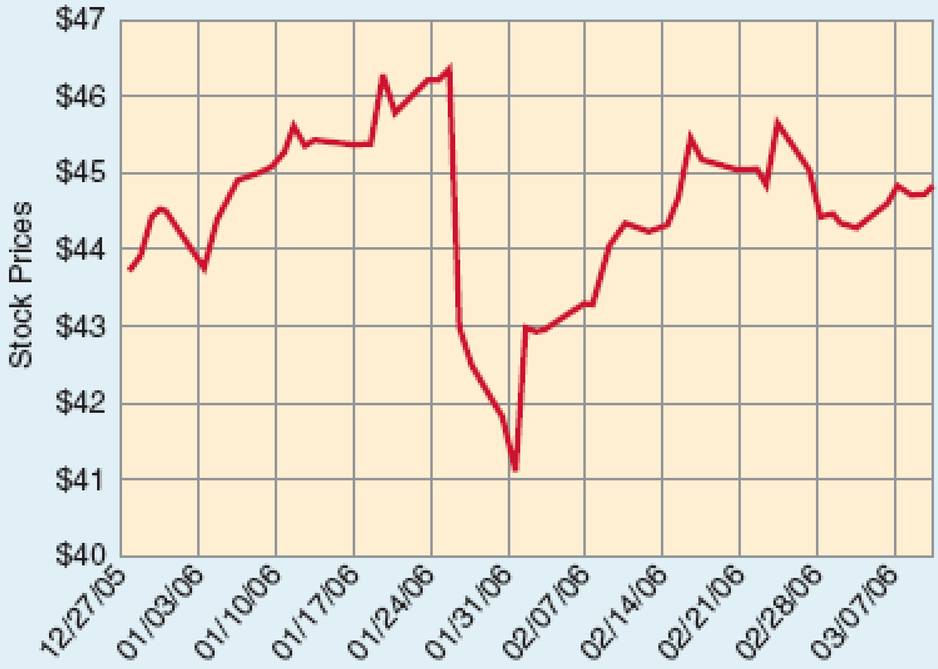


Figure 16.1 Stock market reacts to ChoicePoint's $15 million settlement for data breach.

IS Vulnerability

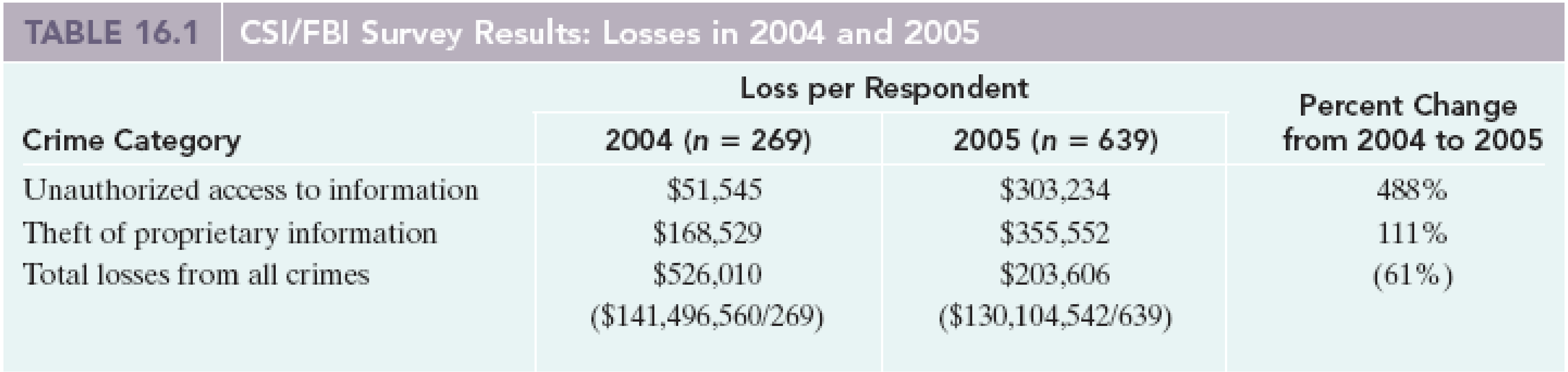
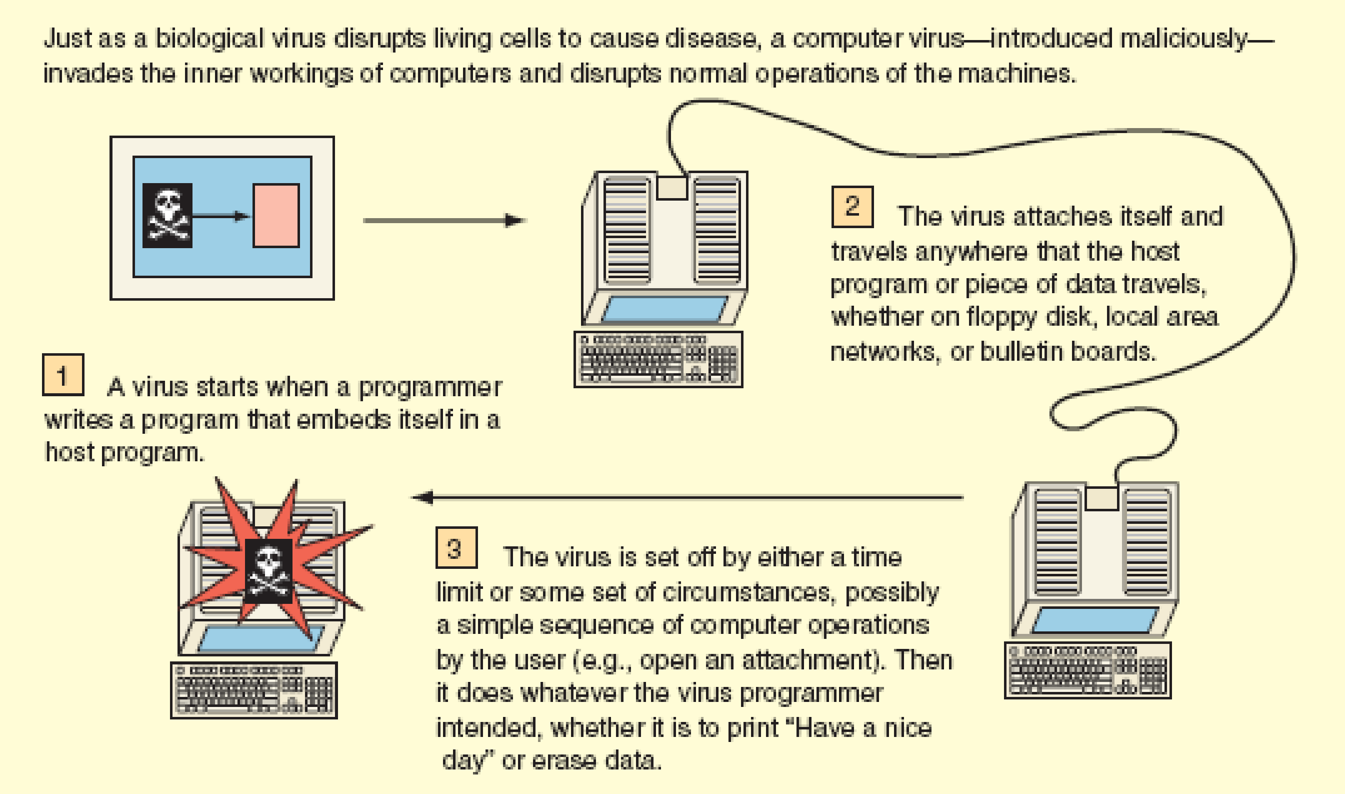


TABLE 16.1 CSI/FBI Survey Results: Losses in 2004 and 2005

Crime Category	Loss per Respondent		Percent Change from 2004 to 2005
	2004 (*n* = 269)	2005 (*n* = 639)	
Unauthorized access to information	$51,545	$303,234	488%
Theft of proprietary information	$168,529	$355,552	111%
Total losses from all crimes	$526,010 ($141,496,560/269)	$203,606 ($130,104,542/639)	(61%)

How a virus works



Just as a biological virus disrupts living cells to cause disease, a computer virus—introduced maliciously—invades the inner workings of computers and disrupts normal operations of the machines.

1 A virus starts when a programmer writes a program that embeds itself in a host program.

2 The virus attaches itself and travels anywhere that the host program or piece of data travels, whether on floppy disk, local area networks, or bulletin boards.

3 The virus is set off by either a time limit or some set of circumstances, possibly a simple sequence of computer operations by the user (e.g., open an attachment). Then it does whatever the virus programmer intended, whether it is to print "Have a nice day" or erase data.

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.

System Vulnerability

- A universal vulnerability is a state in a computing system which either: allows an attacker to execute commands as another user; allows an attacker to access data that is contrary to the access restrictions for that data; allows an attacker to pose as another entity; or allows an attacker to conduct a denial of service.
- An exposure is a state in a computing system (or set of systems) which is not a universal vulnerability, but either: allows an attacker to conduct information gathering activities; allows an attacker to hide activities; includes a capability that behaves as expected, but can be easily compromised; is a primary point of entry that an attacker may attempt to use to gain access to the system or data; and is considered a problem according to some reasonable security policy.

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.
- **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.
- **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.

Information Extortion

- When an attacker or formerly trusted employee steal information from a computer system and then demands compensation for its return or an agreement not to disclose it.

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 progams 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.

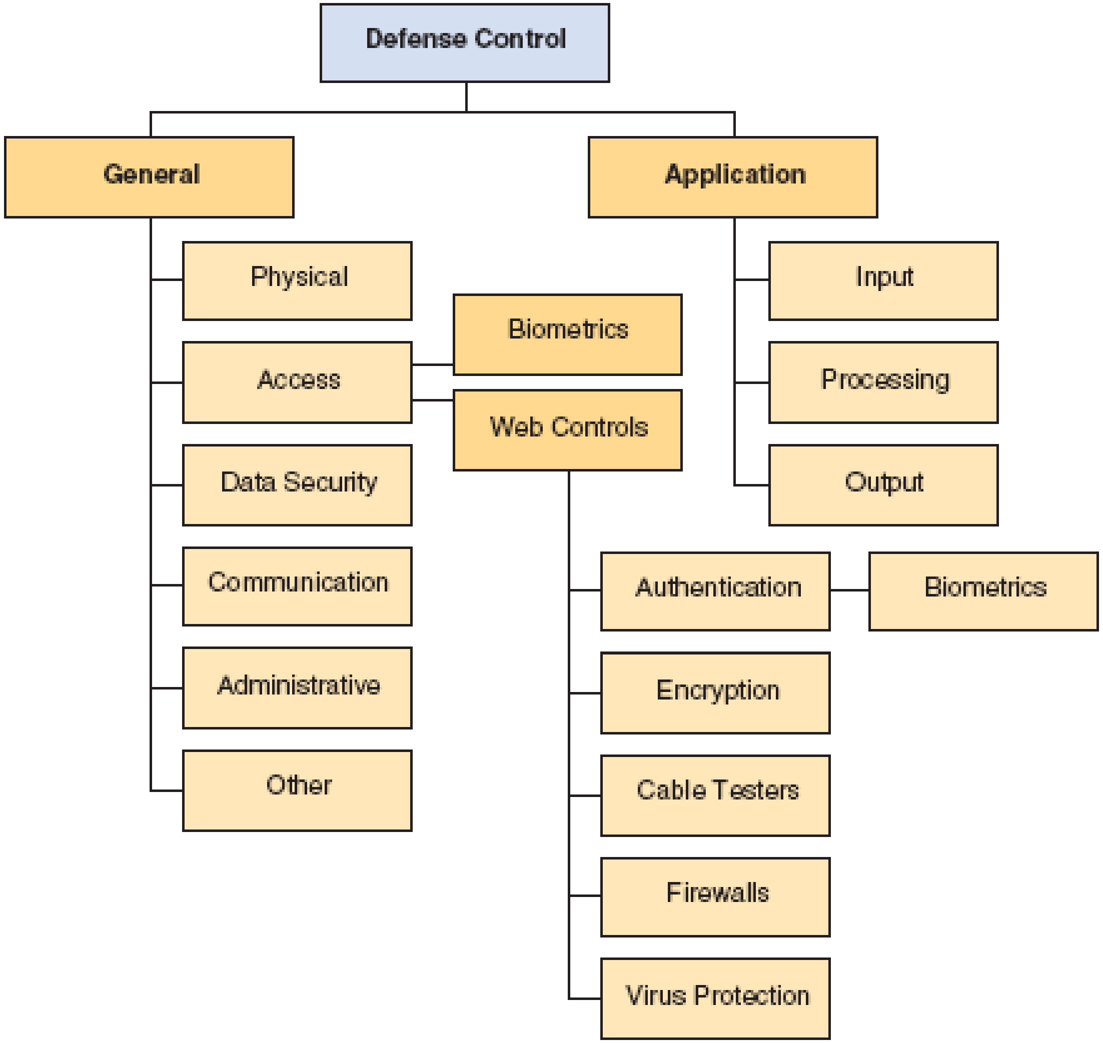
Compromises to Intellectual Property

- **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.

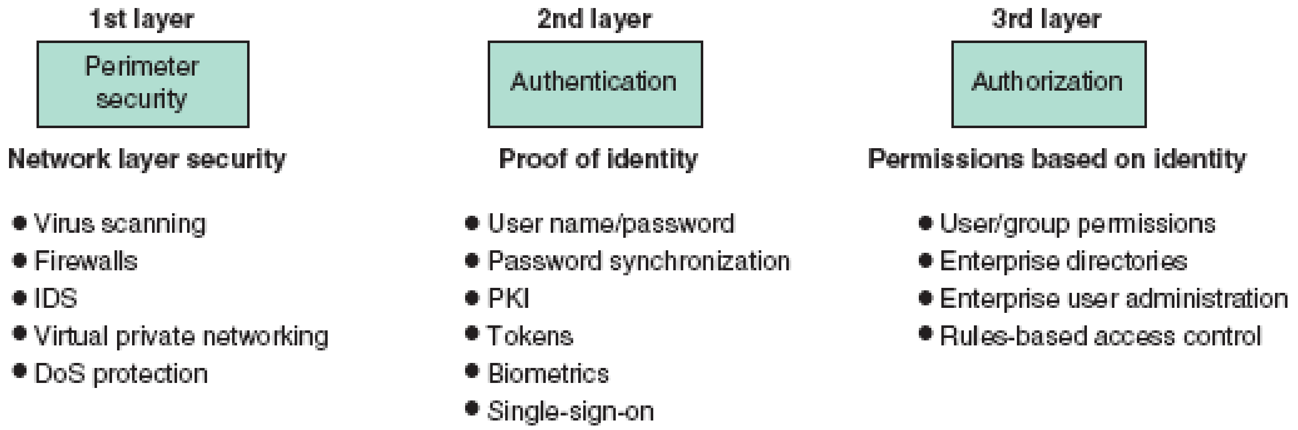
Compromises to Intellectual Property (Continued)

- **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.

Corporate Security Plan - Protecting



Defense Strategy - Controls



1st layer

Perimeter security

Network layer security

- Virus scanning
- Firewalls
- IDS
- Virtual private networking
- DoS protection

2nd layer

Authentication

Proof of identity

- User name/password
- Password synchronization
- PKI
- Tokens
- Biometrics
- Single-sign-on

3rd layer

Authorization

Permissions based on identity

- User/group permissions
- Enterprise directories
- Enterprise user administration
- Rules-based access control

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.

IS Auditing Procedure

- ***Auditing around the computer*** means verifying processing by checking for known outputs or specific inputs.
- ***Auditing through the computer*** means inputs, outputs and processing are checked.
- ***Auditing with the computer*** means using a combination of client data, auditor software, and client and auditor hardware.

Auditing

Implementing controls in an organization can be very complicated and difficult to enforce. Are controls installed as intended? Are they effective? Did any breach of security occur? These and other questions need to be answered by independent and unbiased observers. Such observers perform an auditing task.

- There are two types of auditors:
  - An internal auditor is usually a corporate employee who is not a member of the ISD.
  - An external auditor is a corporate outsider. This type of auditor reviews the findings of the internal audit.
- There are two types of audits.
  - The operational audit determines whether the ISD is working properly.
  - The compliance audit determines whether controls have been implemented properly and are adequate.

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.

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.

Business Continuity

An important element in any security system is the business continuity plan, also known as the disaster recovery plan**.** Such a plan outlines the process by which businesses should recover from a major disaster.

- The purpose of a business continuity plan is to keep the business running after a disaster occurs.
- Recovery planning is part of asset protection*.*
- Planning should focus on recovery from a total loss of all capabilities.
- Proof of capability usually involves some kind of what-if analysis that shows that the recovery plan is current.
- All critical applications must be identified and their recovery procedures addressed.
- The plan should be written so that it will be effective in case of disaster.

Managerial Issues

- What is the business value of IT security and control?
- Why are these legal obligations?
- How important is IT security to management
- IT security and internal control must be implemented top-down
- Acceptable use policies

Managerial Issues (Continued)

- Digital assets are relied upon for competitive advantage
- What does risk management involve
- What are the impacts of IT security breaches
- Federal and State regulations
- Internal Control and Computer Forensics

Chapter 16

Copyright © 2008 John Wiley & Sons, Inc. All rights reserved. Reproduction or translation of this work beyond that permitted in Section 117 of the 1976 United States Copyright Act without the express written permission of the copyright owner is unlawful. Request for further information should be addressed to the Permissions Department, John Wiley & Sons, Inc. The purchaser may make back-up copies for his/her own use only and not for distribution or resale. The Publisher assumes no responsibility for errors, omissions, or damages, caused by the use of these programs or from the use of the information contained herein.