REPUBLIC OF THE PHILIPPINES
POLYTECHNIC UNIVERSITY OF THE PHILIPPINES
STA. MESA, MANILA
COLLEGE OF ENGINEERING
COMPUTER ENGINEERING DEPARTMENT

CMPE 30202

CpE LAWS and PROFESSIONAL PRACTICE

INSTRUCTIONAL MATERIAL

DR. ANTONIO Y. VELASCO

Chapter 1: An Overview of Ethics and Laws

Objectives

As we discuss this chapter, consider the following questions:

- What is ethics, and why is it important to act according to a code of ethics?
- Why is business ethics becoming increasingly important?
- What are organizations doing to improve their business ethics and laws?
- Why are organizations interested in fostering good business ethics and laws ?
- What approach can you take to ensure ethical decision making?
- What trends have increased the risk of using information technology in an unethical manner and IT laws in the course of computer engineering?

What is Ethics?

- Moral code
  - Set of rules
  - Establishes boundaries of generally accepted behavior
  - Different rules often have contradictions
- Morality
  - Social conventions about right and wrong
  - Widely shared
  - Form basis for an established consensus
- Morality may vary by:
  - Age
  - Cultural group
  - Ethnic background
  - Religion
  - Life experiences
  - Education
  - Gender

Definition of Ethics

- Ethics
  - Set of beliefs about right and wrong behavior
- Virtues

    - Habits that incline people to do what is acceptable
- Vices
    - Habits of unacceptable behavior

- Virtues and vices define a personal value system
    - Scheme of moral values

What is Laws?

- System of Rules
    - Set of rules
    - Establishes boundaries
    - Recognizes as regulating actions
- Enforced by a controlling authority
    - Binding
    - Enforced
    - rules
- Enforce by the imposition of penalties
    - customs
    - l practices
    - uphold
    - interpret
    - apply the law

Definition of IT Laws?

- Intellectual Property
    - Set of beliefs about right and wrong behavior
- Contract Law
    - Habits that incline people to do what is acceptable
- privacy
    - Habits of unacceptable behavior
- Freedom of expression
    - Scheme of moral values
    - Jurisdiction

The Importance of Integrity

- Integrity is a cornerstone of ethical behavior

People wit

The Importance of Integrity

- Integrity is a cornerstone of ethical behavior
- People with integrity:
  - Act in accordance with a personal code of principles
  - Extend to all the same respect and consideration
  - Apply the same moral standards in all situations
- Lack of integrity emerges if you apply moral standards differently according to situation or people involved
- Many ethical dilemmas are not as simple as right versus wrong

The Difference Between Morals, Ethics, and Laws

- Morals: one's personal beliefs about right and wrong
- Ethics: standards or codes of behavior expected of an individual by a group
- Law: system of rules that tells us what we can and cannot do
  - Laws are enforced by a set of institutions
  - Legal acts conform to the law
  - Moral acts conform to what an individual believes is the right belief of right and wrong

Ethics in the Business World

- Both the likelihood and the negative impact of inappropriate behavior have increased
- Several trends have increased the likelihood of unethical behavior:
  - Globalization creating complex work environments
  - Organizations challenged to maintain profits / revenue
  - Heightened vigilance by:
    - Employees
    - Shareholders
    - Regulatory agencies
    -
- Recent scandals in IT companies
  - Satyam Computer Services (India)
  - Hewlett Packard
  - Computer Associates International
  - IBM

- Not just executives, but even lower-level employees, can find themselves in the middle of an ethical dilemma

Why Fostering Good Business Ethics Is Important

- To gain the good will of the community
- To create an organization that operates consistently
- To foster good business practices
- To protect organization/employees from legal action
- To avoid unfavorable publicity

Gaining the Good Will of the Community

- Organizations have fundamental responsibilities to society
  - Declared in formal statement of company's principles or beliefs
  - Include:
    - Making contributions to charitable organizations and nonprofit institutions
    - Providing benefits for employees in excess of legal requirements
    - Choosing economic opportunities that might be more socially desirable than profitable
- Socially responsible activities create good will
- Good will makes it easier for corporations to conduct business

Creating an Organization That Operates Consistently

- Consistency ensures that employees:
  - Know what is expected of them
  - Can employ the organization's values to help them in decision making
- Consistency also means that shareholders, customers, suppliers, and community know what they can expect of the organization
- Many companies share the following values:
  - Operate with honesty and integrity, staying true to organizational principles
  - Operate according to standards of ethical conduct, in words and action
  - Treat colleagues, customers, and consumers with respect
  - Strive to be the best at what matters to the company
  - Value diversity
  - Make decisions based on facts and principles

Fostering Good Business Practices

- Good ethics means good business/improved profits
- Companies that:
  - Produce safe and effective products
  - Avoid costly recalls and lawsuits
  - Provide excellent service that retains customers
  - Develop and maintain strong employee relations
    - Suffer lower turnover rates
    - Enjoy better employee morale
- Suppliers/business partners place priority on working with companies that operate in a fair and ethical manner
- Bad ethics means bad business/waning profits
  - Bad ethics can lead to bad business results
  - Bad ethics can have a negative impact on employees

Protecting the Organization and Its Employees from Legal Actions

- U.S. Supreme Court established that an employer can be held responsible for the acts of its employees
- This principle is called "*respondeat superior"*
- Coalition of several legal organizations argues establishment of ethics and compliance programs should reduce criminal liability of organization
- Others argue company officers should not be given light sentences if their ethics programs are ineffective

Avoiding Unfavorable Publicity

- Public reputation of company strongly influences:
  - Value of its stock
  - How consumers regard products and services
  - Degree of oversight received from government
  - Amount of support and cooperation received
- Organizations are motivated to build strong ethics programs to avoid negative publicity

Improving Corporate Ethics

Characteristics of a successful ethics program

- Employees willing to seek advice about ethical issues

- Employees feel prepared to handle situations that could lead to misconduct
- Employees are rewarded for ethical behavior
- Employees are not rewarded for success obtained through questionable means
- Employees feel positive about their company

Appointing a Corporate Ethics Officer

Corporate ethics officer

- Provides vision and leadership in business conduct
- Should be well-respected, senior-level manager who reports directly to the CEO
- Ensures ethical procedures are put in place
- Creates and maintains ethics culture
- Is responsible for key knowledge/contact person for ethical issues

Ethical Standards Set by Board of Directors

- Board oversees the organization's business activities and management
- Board members of company are expected to:
  - Conduct themselves according to the highest standards of personal and professional integrity
  - Set standard for company-wide ethical conduct
  - Ensure compliance with laws and regulations
  - Create environment in which employees can seek advice about business conduct, raise issues, and report misconduct

Establishing a Corporate Code of Ethics

- Code of ethics
  - Highlights an organization's key ethical issues
  - Identifies overarching values and important principles
  - Focuses employees on areas of ethical risk
  - Offers guidance for employees to recognize and deal with ethical issues
  - Provides mechanisms to report unethical conduct
  - Help employees abide by the law, follow necessary regulations, and behave in an ethical manner
- Sarbanes-Oxley Act of 2002
  - Enacted in response to public outrage over several major accounting scandals

- Section 404 requires that the CEO and CFO sign any SEC filing to attest to its accuracy
- Section 406 requires public companies to disclose whether or not they have a code of ethics and if any waivers to that code have been granted
- Cannot gain company-wide acceptance unless it is:
  - Developed with employee participation
  - Fully endorsed by organization's leadership
- Must continually be applied to company's decision making and emphasized as part of its culture
- Breaches in the code of ethics must be identified and dealt with appropriately

1. Intel conducts business with honesty and integrity
2. Intel follows the letter and spirit of the law
3. Intel employees treat each other fairly
4. Intel employees act in the best interests of Intel and avoid conflicts of interest
5. Intel employees protect the company's assets and reputation

FIGURE 1-4 Intel's five principles of conduct

Credit: Five Principals of Conduct. © Intel Corporation. Reprinted by permission.

Conducting Social Audits

- Social audit
  - Reviews how well organization is meeting ethical and social responsibility goals
  - Communicates new goals for upcoming year
  - Shared broadly with employees, shareholders, investors, market analysts, customers, suppliers, government agencies, and local communities

Requiring Employees to Take Ethics Training

- Personal convictions improved through education
- Comprehensive ethics education program encourages employees to act responsibly and ethically
  - Often presented in small workshop formats
  - Employees apply code of ethics to hypothetical but realistic case studies
  - Demonstration of recent company decisions based on principles from the code of ethics
- Critical training increase the percentage of employees who report incidents of misconduct
- Employees must:

- Learn effective ways of reporting incidents
- Be reassured their feedback will be acted on without retaliation

Including Ethical Criteria in Employee Appraisals

- Good employees may make bad ethical choices
- May be encouraged to do "whatever it takes" to get the job done
- Employees need a knowledgeable resource to discuss perceived unethical practices
  - A manager
  - Legal or Internal Audit Department
  - Business Unit's legal counsel
  - Anonymously through internal Web site

TABLE 1-3 Manager's checklist for establishing an ethical work environment

Question	Yes	No
Does your organization have a code of ethics?		
Do employees know how and to whom to report any infractions of the code of ethics?		
Do employees feel that they can report violations of the code of ethics safely and without fear of retaliation?		
Do employees feel that action will be taken against those who violate the code of ethics?		
Do senior managers set an example by communicating the code of ethics and using it in their own decision making?		
Do managers evaluate and provide feedback to employees on how they operate with respect to the values and principles in the code of ethics?		
Are employees aware of sanctions for breaching the code of ethics?		
Do employees use the code of ethics in their decision making?		

Source Line: Course Technology/Cengage Learning.

Including Ethical Considerations in Decision Making

Steps in a decision-making process

- Develop problem statement
- Identify alternatives
- Evaluate and choose alternative
- Implement decision
- Evaluate results
- Success

Develop a Problem Statement

- Clear, concise description of the issue
- Answers these questions:
  - What causes people to think there is a problem?
  - Who is directly affected by the problem?
  - Is there anyone else affected?
  - How often does it occur?
  - What is the impact of the problem?
  - How serious is the problem?
- Most critical step in decision-making process
- Example of a good problem statement:
  - "Our product supply organization is continually running out of stock of finished products, creating an out-of-stock situation on over 15 percent of our customer orders, resulting in over $300,000 in lost sales per month."
- Examples of poor problem statements:
  - "We need to implement a new inventory control system." (possible solution, not a problem statement)
  - "We have a problem with finished product inventory." (not specific enough)

Identify, Evaluate, and Choose an Alternative

- Enlist help to brainstorm alternative solutions
- Evaluate by weighing laws, guidelines, and principles
- Consider likely consequences of each alternative
- Alternative selected must:
  - Be ethically and legally defensible
  - Be consistent with policies and code of ethics
  - Take into account impact on others
  - Provide a good solution to problem

TABLE 1-4 Four common approaches to ethical decision making

Approach to dealing with moral issues	Principle
Virtue ethics approach	The ethical choice best reflects moral virtues in yourself and your community.
Utilitarian approach	The ethical choice produces the greatest excess of benefits over harm.
Fairness approach	The ethical choice treats everyone the same and shows no favoritism or discrimination.
Common good approach	The ethical choice advances the common good.

Source Line: Course Technology/Cengage Learning.

Virtue Ethics Approach

- Virtue ethics approach
  - Focuses on concern with daily life in a community
  - People guided by virtues to reach “right” decision
  - More effective than following set of principles/rules
- Problems
  - Does not provide guide for action
  - Virtue cannot be worked out objectively; depends on circumstances

Utilitarian Approach

- Utilitarian approach
  - Chooses action that has best overall consequences
  - Finds the greatest good by balancing all interests
  - Fits concept of value in economics and the use of cost-benefit analysis
- Problems
  - Measuring and comparing values is often difficult
  - Predicting resulting benefits and harm is difficult

Fairness Approach

- Fairness approach
  - Focuses on fair distribution of benefits/burdens
  - Guiding principle is to treat all people the same
- Problems
  - Decisions can be influenced by personal bias
  - Others may consider the decision unfair

Common Good Approach

- Common good approach
  - Work together for common set of values and goals
  - Implement systems that benefit all people
- Problems
  - Consensus is difficult
  - Some required to bear greater costs than others

Implement the Decision and Evaluate the Results

- Implement the decision

    - Efficient, effective, timely implementation
    - Communication is key for people to accept change
    - Transition plan made easy and pain-free
- Evaluate the results
    - Monitor results for desired effect
    - Observe impact on organization and stakeholders
    - Return to “Develop problem statement” step if further refinements may be needed

Ethics in Information Technology

- Public concern about the ethical use of information technology includes:
    - E-mail and Internet access monitoring
    - Downloading in violation of copyright laws
    - Unsolicited e-mail (spam)
    - Hackers and identify theft
    - Students and plagiarism
    - Cookies and spyware
- The general public does not understand the critical importance of ethics as applied to IT
- Important decisions are often left to technical experts
- General business managers must assume greater responsibility for these decisions by:
    - Making decisions based on technical savvy, business know-how, and a sense of ethics
    - Creating an environment where ethical dilemmas can be discussed openly, objectively, and constructively

- Goals of this text
    - To educate people about the tremendous impact of ethical issues in the successful and secure use of information technology
    - To motivate people to recognize these issues when making business decisions
    - To provide tools, approaches, and useful insights for making ethical decisions

Summary

- Ethics is important because the risks associated with inappropriate behavior have increased

- Organizations have at least five good reasons for encouraging employees to act ethically
  - To gain the good will of the community
  - To create an organization that operates consistently
  - To foster good business practices
  - To protect the organization and its employees against legal action
  - To avoid unfavorable publicity
- Organizations require successful ethics programs
- The corporate ethics officer ensures that ethical procedures are installed and followed
- Managers' behaviors and expectations can strongly influence employees' ethical behavior
- Most of us have developed a simple decision-making model that includes five steps
- Ethical considerations must be incorporated into decision making
- Four common approaches to ethical decision making
  - Virtue ethics approach
  - Utilitarian approach
  - Fairness approach
  - Common good approach

Activity 1.

Directions: Answer the following questions with True or False before the number.

_____1. Morality in ethics does not change and is constant through cultures.

_____2. Vices are habits that incline people to do what is acceptable.

_____3. Nowadays, the likelihood and the negative impact of inappropriate behavior have increased.

_____4. Good will makes it easier for corporations to conduct business.

_____5. Suppliers/business partners should not place priority on working with companies that operate in a fair and ethical manner.

_____6. U.S. Supreme Court established that an employer is not responsible for the acts of its employees.

_____7. Improving corporate ethics include employees are rewarded for success obtained through questionable means.

_____8. Corporate ethics officer is responsible for key knowledge/contact person for ethical issues.

_____9. Critical training increase the percentage of employees who report incidents of misconduct.

_____10. A problem statement should be short and precise.

Chapter 2: Ethics for IT Workers and IT Users

Objectives

As you read this chapter, consider the following questions:

- What key characteristics distinguish a professional from other kinds of workers, and is an IT worker considered a professional?
- What factors are transforming the professional services industry?
- What relationships must an IT worker manage, and what key ethical issues can arise in each?
- How do codes of ethics, professional organizations, certification, and licensing affect the ethical behavior of IT professionals?
- What is meant by compliance, and how does it help promote the right behaviors and discourage undesirable ones?

IT Professionals

- Profession is a calling that requires specialized knowledge and long and intensive academic preparation
- Professionals are people that require advanced training and experience, must exercise discretion and judgment in their work, their work cannot be

standardized, must contribute to society, participate in lifelong training, assist other professionals and carry special rights and responsibilities

Are IT Workers Professionals?

- Partial list of IT specialists
  - Programmers
  - Systems analysts
  - Software engineers
  - Database administrators
  - Local area network (LAN) administrators
  - Chief information officers (CIOs)
- Legal perspective
  - IT workers do not meet legal definition of professional
  - Not licensed by state or federal government
  - Not liable for malpractice
  -

The Changing Professional Services Industry

- IT workers are considered part of the professional services industry
- Seven forces are changing professional services
  - Client sophistication (able to drive hard bargains)
  - Governance (due to major scandals)
  - Connectivity (instant communications)
  - Transparency (view work-in-progress in real-time)
  - Modularization (able to outsource modules)
  - Globalization (worldwide sourcing)
  - Commoditization (for low-end services)

Professional Relationships That Must Be Managed

IT workers involved in relationships with:

- Employers
- Clients
- Suppliers
- Other professionals
- IT users
- Society at large

Relationships Between IT Workers and Employers

- IT workers agree on many aspects of work relationship before workers accept job offer
- Other aspects of work relationship defined in company's policy and procedure manual or code of conduct
- Some aspects develop over time
- As steward of organization's IT resources, IT workers must set an example and enforce policies regarding the ethical use of IT in:
- Software piracy
  - Act of illegally making copies of software or enabling access to software to which they are not entitled
  - Area in which IT workers can be tempted to violate laws and policies
  - The Business Software Alliance (BSA) is a trade group representing the world's largest software and hardware manufacturers; mission is to stop the unauthorized copying of software
  - Thousands of cases prosecuted each year

TABLE 2-1 Worldwide and policy council members of Business Software Alliance (as of November 2010)

Adobe	Altium	Apple	Autodesk
AVEVA	AVG	Bentley Systems	CA
Cadence Design Systems	Cisco Systems	CNC Software–Mastercam	Corel
Dassault Systèmes SolidWorks Corporation	Dell	HP	IBM
Intel	Intuit	Kaspersky	McAfee
Microsoft	Mindjet	Progress Software	PTC
Quark	Quest	Rockwell Automation	Siemens PLM Software, Inc.
Stone Bond Technologies	Sybase	Symantec	Synopsys

Source Line: Business Software Alliance, "BSA Members," © 2011, www.bsa.org/country/BSA%20and%20Members/Our%20Members.aspx.

- IT workers must set an example and enforce policies regarding the ethical use of IT in: (cont'd.)
  - Trade secrets
    - Business information generally unknown to public
    - Company takes actions to keep confidential
    - Require cost or effort to develop
    - Have some degree of uniqueness or novelty
  - Whistle-blowing

    - Employee attracts attention to a negligent, illegal, unethical, abusive, or dangerous act that threatens the public interest

Relationships Between IT Workers and Clients

- IT worker provides:
  - Hardware, software, or services at a certain cost and within a given time frame
- Client provides:
  - Compensation
  - Access to key contacts
  - Work space
- Relationship is usually documented in contractual terms
- Client makes decisions about a project based on information, alternatives, and recommendations provided by the IT worker
- Client trusts IT worker to act in client's best interests
- IT worker trusts that client will provide relevant information, listen to and understand what the IT worker says, ask questions to understand impact of key decisions, and use the information to make wise choices
- Ethical problems arise if a company recommends its own products and services to remedy problems they have detected
  - Creates a conflict of interest
- Problems arise during a project if IT workers are unable to provide full and accurate reporting of a project's status
  - Finger pointing and heated discussions can ensue
- Fraud
  - Crime of obtaining goods, services, or property through deception or trickery
- Misrepresentation
  - Misstatement or incomplete statement of material fact
  - If misrepresentation causes a party to enter into a contract, that party may have the right to cancel contract or seek reimbursement for damages
- Breach of contract
  - One party fails to meet the terms of a contract
  - When there is material breach of contract:
    - The non-breaching party may rescind the contract, seek restitution of any compensation paid to the breaching party, and be discharged from any further performance under the contract
- IT projects are joint efforts in which vendors and customers work together
  - When there are problems, it is difficult to assign who is at fault

Relationships Between IT Workers and Suppliers

- Develop good working relationships with suppliers:
  - To encourage flow of useful information and ideas to develop innovative and cost-effective ways of using the supplier in ways that the IT worker may not have considered
  - By dealing fairly with them
  - By not making unreasonable demands
- Bribery
  - Providing money, property, or favors to obtain a business advantage
  - U.S. Foreign Corrupt Practices Act (FCPA): crime to bribe a foreign official, a foreign political party official, or a candidate for foreign political office
  - At what point does a gift become a bribe?
  - No gift should be hidden
  - Perceptions of donor and recipient can differ
  - United Nations Convention Against Corruption is a global treaty to fight bribery and corruption

TABLE 2-2 Distinguishing between bribes and gifts

Bribes	Gifts
Are made in secret, as they are neither legally nor morally acceptable	Are made openly and publicly, as a gesture of friendship or goodwill
Are often made indirectly through a third party	Are made directly from donor to recipient
Encourage an obligation for the recipient to act favorably toward the donor	Come with no expectation of a future favor for the donor

Source Line: Course Technology/Cengage Learning.

Relationships Between IT Workers and Other Professionals

- Professionals feel a degree of loyalty to other members of their profession
- Professionals owe each other adherence to their profession's code of conduct
- Ethical problems among the IT profession
  - Résumé inflation on 30% of U.S. job applications
  - Inappropriate sharing of corporate information
    - Information might be sold intentionally or shared informally with those who have no need to know

Relationships Between IT Workers and IT Users

- IT user: person using a hardware or software product
- IT workers' duties
  - Understand users' needs and capabilities
  - Deliver products and services that meet those needs
  - Establish environment that supports ethical behavior:
    - To discourages software piracy
    - To minimize inappropriate use of corporate computing resources
    - To avoid inappropriate sharing of information

Relationships Between IT Workers and Society

- Society expects members of a profession:
  - To provide significant benefits
  - To not cause harm through their actions
- Actions of an IT worker can affect society
- Professional organizations provide codes of ethics to guide IT workers' actions

Professional Codes of Ethics

- State the principles and core values that are essential to the work of an occupational group
- Most codes of ethics include:
  - What the organization aspires to become
  - Rules and principles by which members of the organization are expected to abide
- Many codes also include commitment to continuing education for those who practice the profession
- Following a professional code of ethics can produce benefits for the individual, the profession, and society as a whole
  - Ethical decision making
  - High standards of practice and ethical behavior
  - Trust and respect from general public
  - Evaluation benchmark for self-assessment

Professional Organizations

- No universal code of ethics for IT professionals
- No single, formal organization of IT professionals has emerged as preeminent

- Five of the most prominent organizations include:
  - Association for Computing Machinery (ACM)
  - Institute of Electrical and Electronics Engineers Computer Society (IEEE-CS)
  - Association of IT Professionals (AITP)
  - SysAdmin, Audit, Network, Security (SANS) Institute

Certification

- Indicates that a professional possesses a particular set of skills, knowledge, or abilities in the opinion of the certifying organization
- Can also apply to products
- Generally, voluntary
- May or may not require adherence to a code of ethics
- Employers view as benchmark of knowledge
- Opinions are divided on value of certification
- Vendor certifications
  - Some certifications substantially improve IT workers' salaries and career prospects
  - Relevant for narrowly defined roles or certain aspects of broader roles
  - Require passing a written exam, or in some cases, a hands-on lab to demonstrate skills and knowledge
  - Can take years to obtain necessary experience
  - Training can be expensive
- Industry association certifications
  - Require a higher level of experience and a broader perspective than vendor certifications
  - Must sit for and pass written exam
  - May need to pay annual renewal fee, earn continuing education credits, and/or pass renewal test
  - Lag in developing tests that cover new technologies
  - Are moving from purely technical content to a broader mix of technical, business, and behavioral competencies

Government Licensing

- License is a government-issued permission to engage in an activity or operate a business
- Generally administered at the state level in the United States
- Often requires that recipient pass a test

- Some professionals must be licensed – doctors, lawyers, CPAs, medical and day care providers, engineers
- One goal: protect public safety
- Case for licensing IT workers
  - Encourages following highest standards of profession
  - Encourages practicing a code of ethics
  - Violators would be punished
- Without licensing, there are no requirements for heightened care and no concept of professional malpractice
- Issues associated with government licensing of IT workers
  - There are few licensing programs for IT professionals
    - No universally accepted core body of knowledge
    - Unclear who should manage content and administration of licensing exams
    - No administrative body to accredit professional education programs
    - No administrative body to assess and ensure competence of individual workers

IT Professional Malpractice

- Negligence: not doing something that a reasonable person would do, or doing something that a reasonable person would not do
- Duty of care: obligation to protect people against any unreasonable harm or risk
  - Reasonable person standard
  - Reasonable professional standard
- Professional malpractice: professionals who breach the duty of care are liable for injuries that their negligence causes

IT Users

- Employees' ethical use of IT is an area of growing concern because of increased access to:
  - Personal computers
  - Corporate information systems and data
  - The Internet

Common Ethical Issues for IT Users

- Software piracy
- Inappropriate use of computing resources
  - Erodes productivity and wastes time
  - Could lead to lawsuits
- Inappropriate sharing of information, including:
  - Every organization stores vast amounts of private or confidential data
    - Private data (employees and customers)
    - Confidential information (company and operations)

Supporting the Ethical Practices of IT Users

- Policies that protect against abuses:
  - Set forth general rights and responsibilities of users
  - Create boundaries of acceptable behaviour
  - Enable management to punish violators
- Policy components include:
  - Establishing guidelines for use of company software
  - Defining appropriate use of IT resources
  - Structuring information systems to protect data and information
  - Installing and maintaining a corporate firewall

TABLE 2-5 Manager's checklist for establishing an IT usage policy

Question	Yes	No
Is there a statement that explains the need for an IT usage policy?		
Does the policy provide a clear set of guiding principles for ethical decision making?		
Is it clear how the policy applies to the following types of workers? • Employees • Part-time workers • Temps • Contractors		

Does the policy address the following issues? • Protection of the data privacy rights of employees, customers, suppliers, and others • Control of access to proprietary company data and information • Use of unauthorized or pirated software • Employee monitoring, including email, wiretapping and eavesdropping on phone conversations, computer monitoring, and surveillance by video • Respect of the intellectual rights of others, including trade secrets, copyrights, patents, and trademarks • Inappropriate use of IT resources, such as Web surfing, personal emailing, and other use of computers for purposes other than business • The need to protect the security of IT resources through adherence to good security practices, such as not sharing user IDs and passwords, using "hard-to-guess" passwords, and frequently changing passwords • The use of the computer to intimidate, harass, or insult others through abusive language in emails and by other means
Are disciplinary actions defined for IT-related abuses?
Is there a process for communicating the policy to employees?
Is there a plan to provide effective, ongoing training relative to the policy?
Has a corporate firewall been implemented?
Is the corporate firewall maintained?

Source Line: Course Technology/Cengage Learning.

Compliance

- To be in accordance with established policies, guidelines, specifications, and legislation
  - Sarbanes-Oxley – established requirements for internal controls
  - HIPAA – ensures security and privacy of employee healthcare data
  - Failure to be in conformance can lead to criminal or civil penalties and also lawsuits
- Major challenge to comply with multiple government and industry regulations that are sometimes in conflict
- To meet this challenge:
  - Implement software to track and record compliance actions

    - Hire management consultants for advice and training
    - Create Chief Compliance Officer position
- Audit committee is subset of the board of directors, with oversight for the following activities:
    - Quality and integrity of accounting and reporting practices and controls
    - Compliance with legal and regulatory requirements
    - Qualifications, independence, and performance of organization's independent auditor
    - Performance of company's internal audit team
- Internal audit committee responsibilities:
    - Determine that internal systems and controls are adequate and effective
    - Verify existence of company assets and maintain proper safeguards over their protection
    - Measure the organization's compliance with its own policies and procedures
    - Insure that institutional policies and procedures, appropriate laws, and good practices are followed
    - Evaluate adequacy and reliability of information available for management decision making

Summary

- Professionals
    - Require advanced training and experience
    - Must exercise discretion and judgment in their work
    - Their work cannot be standardized
- From a legal standpoint, a professional:
    - Has passed the state licensing requirements
    - Has earned the right to practice in a state(s)

- IT professionals have many different relationships
  - Each with its own ethical issues and potential problems
- Professional code of ethics
  - States the principles and core values essential to the work of an occupational group
  - Serves as a guideline for ethical decision making
  - Promotes high standards of practice and behaviour
  - Enhances trust and respect from the general public
  - Provides an evaluation benchmark
- Licensing and certification of IT professionals
  - Would increase the reliability and effectiveness of information systems
  - Raises many issues
- IT-related professional organizations have developed their code of ethics that:
  - Outlines what the organization aspires to become
  - Lists rules and principles for members
  - Includes a commitment to continuing education for those who practice the profession
- Audit committee and internal audit team have a major role in ensuring that both the IT organization and IT users are in compliance with guidelines and various legal and regulatory practices

Activity:

Directions: Fill in the blanks with the correct and most appropriate answer.

1. Professionals should Contribute to _____, participate in lifelong training, and assist other professionals.
2. Other aspects of work relationship is defined in the _____ _____ and procedure manual or code of conduct.
3. As _____ of organization's IT resources, IT workers must set an example and enforce policies regarding the ethical use of IT.
4. _____ is an Act of illegally making copies of software or enabling access to software to which they are not entitled.

5. _____ is a trade group representing the world's largest software and hardware manufacturers; mission is to stop the unauthorized copying of software.
6. A _____ makes decisions about a project based on information, alternatives, and recommendations provided by the IT worker.
7. When one party fails to meet the terms of a contract is called _____.
8. Professional organizations provide _____ to guide IT workers' actions.
9. _____ is a government-issued permission to engage in an activity or operate a business.
10. _____: not doing something that a reasonable person would do, or doing something that a reasonable person would not do.

Chapter 3: Computer and Internet Crime

Objectives

As you read this chapter, consider the following questions:

- What key trade-offs and ethical issues are associated with the safeguarding of data and information systems?
- Why has there been a dramatic increase in the number of computer-related security incidents in recent years?
- What are the most common types of computer security attacks?
- Who are the primary perpetrators of computer crime, and what are their objectives?
- What are the key elements of a multilayer process for managing security vulnerabilities based on the concept of reasonable assurance?
- What actions must be taken in response to a security incident?
- What is computer forensics, and what role does it play in responding to a computer incident?

IT Security Incidents: A Major Concern

- Security of information technology is of utmost importance
  - Safeguard:
    - Confidential business data
    - Private customer and employee data
  - Protect against malicious acts of theft or disruption
  - Balance against other business needs and issues
- Number of IT-related security incidents is increasing around the world

Why Computer Incidents Are So Prevalent

- Increasing complexity increases vulnerability
  - Computing environment is enormously complex
    - Continues to increase in complexity
    - Number of entry points expands continuously
    - Cloud computing and virtualization software
- Higher computer user expectations
  - Computer help desks under intense pressure
    - Forget to verify users' IDs or check authorizations
- Computer users share login IDs and passwords
- Expanding/changing systems equal new risks
  - Network era
    - Personal computers connect to networks with millions of other computers
    - All capable of sharing information
  - Information technology
    - Ubiquitous
    - Necessary tool for organizations to achieve goals
    - Increasingly difficult to match pace of technological change
- Increased reliance on commercial software with known vulnerabilities
  - Exploit
    - Attack on information system
    - Takes advantage of system vulnerability
    - Due to poor system design or implementation
  - Patch
    - "Fix" to eliminate the problem
    - Users are responsible for obtaining and installing
    - Delays expose users to security breaches
- Zero-day attack
  - Before a vulnerability is discovered or fixed

- U.S. companies rely on commercial software with known vulnerabilities

Types of Exploits

- Computers as well as smartphones can be target
- Types of attacks
  - Virus
  - Worm
  - Trojan horse
  - Distributed denial of service
  - Rootkit
  - Spam
  - Phishing (spear-phishing, smishing, and vishing)

Viruses

- Pieces of programming code that is usually disguised as something else that causes unexpected and undesirable behavior to the computer and is often attached to files.
- Deliver a “payload”
- Spread by actions of the “infected” computer user
  - Infected e-mail document attachments
  - Downloads of infected programs
  - Visits to infected Web sites

Worms

- Harmful programs that resides in active memory of a computer that duplicate themselves
- Can propagate without human intervention
- Negative impact of worm attack
  - Lost data and programs
  - Lost productivity
  - Additional effort for IT workers

Trojan Horses

- Malicious code hidden inside seemingly harmless programs
- Users are tricked into installing them

- Delivered via email attachment, downloaded from a Web site, or contracted via a removable media device
- Logic bomb
  - Executes when triggered by certain event

Distributed Denial-of-Service (DDoS) Attacks

- Malicious hacker takes over computers on the Internet and causes them to flood a target site with demands for data and other small tasks
  - The computers that are taken over are called zombies
  - Botnet is a very large group of such computers
- Does not involve a break-in at the target computer
  - Target machine is busy responding to a stream of automated requests
  - Legitimate users cannot access target machine

Rootkits

- Set of programs that enables its user to gain administrator-level access to a computer without the end user's consent or knowledge
- Attacker can gain full control of the system and even obscure the presence of the rootkit
- Fundamental problem in detecting a rootkit is that the operating system currently running cannot be trusted to provide valid test results

Spam

- Abuse of email systems to send unsolicited email to large numbers of people
  - Low-cost commercial advertising for questionable products
  - Method of marketing also used by many legitimate organizations
- Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act
  - Legal to spam if basic requirements are met
- Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA)
  - Software generates tests that humans can pass but computer programs cannot

Phishing

- Act of using email fraudulently to try to get the recipient to reveal personal data
- Legitimate-looking emails lead users to counterfeit Web sites
- Spear-phishing
  - Fraudulent emails to an organization's employees
- Smishing
  - Phishing via text messages
- Vishing
  - Phishing via voice mail messages

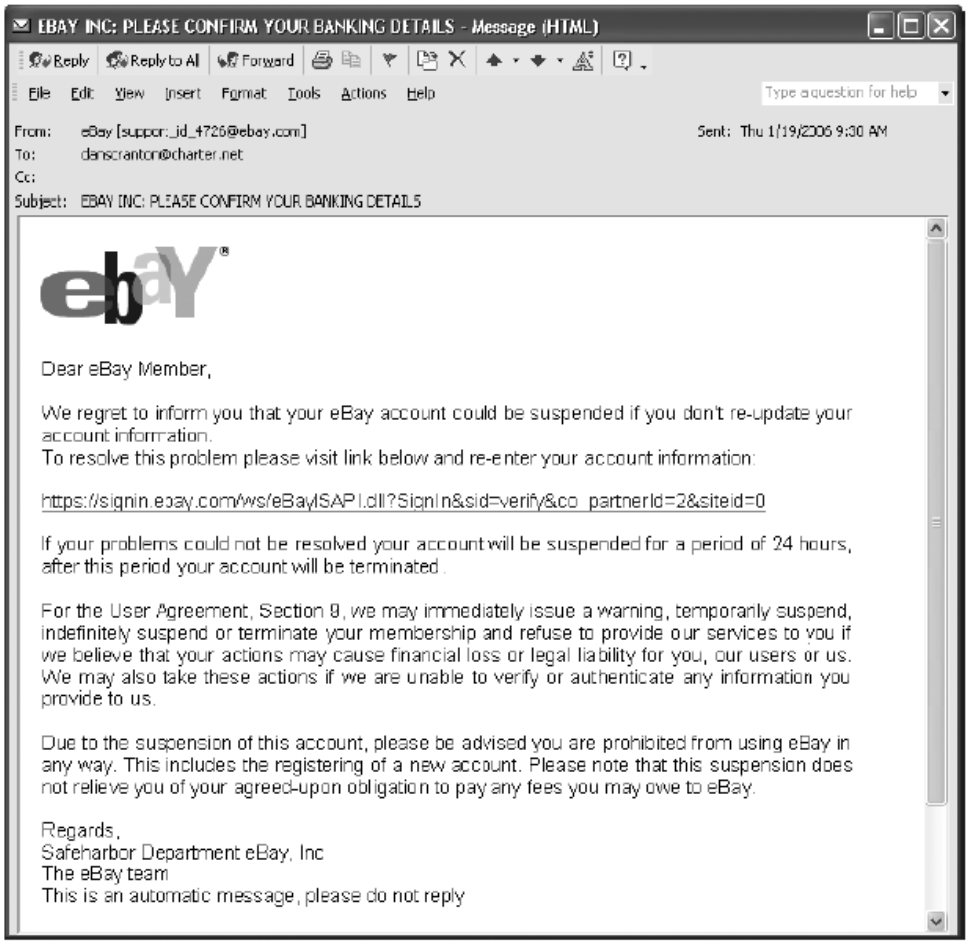

FIGURE 3-3 Example of phishing
Source Line: Course Technology/Cengage Learning.

Types of Perpetrators

- Perpetrators include:
  - Thrill seekers wanting a challenge

    - Common criminals looking for financial gain
    - Industrial spies trying to gain an advantage
    - Terrorists seeking to cause destruction
- Different objectives and access to varying resources
- Willing to take different levels of risk to accomplish an objective

TABLE 3-4 Classifying perpetrators of computer crime

Type of perpetrator	Typical motives
Hacker	Test limits of system and/or gain publicity
Cracker	Cause problems, steal data, and corrupt systems
Malicious insider	Gain financially and/or disrupt company's information systems and business operations
Industrial spy	Capture trade secrets and gain competitive advantage
Cybercriminal	Gain financially
Hacktivist	Promote political ideology
Cyberterrorist	Destroy infrastructure components of financial institutions, utilities, and emergency response units

Source Line: Course Technology/Cengage Learning.

Hackers and Crackers

- Hackers
    - Test limitations of systems out of intellectual curiosity
        - Some smart and talented
        - Others inept; termed "lamers" or "script kiddies"
- Crackers
    - Cracking is a form of hacking
    - Clearly criminal activity

Malicious Insiders

- Major security concern for companies
- Fraud within an organization is usually due to weaknesses in internal control procedures
- Collusion
    - Cooperation between an employee and an outsider
- Insiders are not necessarily employees
    - Can also be consultants and contractors
- Extremely difficult to detect or stop

    - Authorized to access the very systems they abuse
- Negligent insiders have potential to cause damage

Industrial Spies

- Use illegal means to obtain trade secrets from competitors
- Trade secrets are protected by the Economic Espionage Act of 1996
- Competitive intelligence
    - Uses legal techniques
    - Gathers information available to the public
- Industrial espionage
    - Uses illegal means
    - Obtains information not available to the public

Cybercriminals

- Hack into corporate computers to steal
- Engage in all forms of computer fraud
- Chargebacks are disputed transactions
- Loss of customer trust has more impact than fraud
- To reduce potential for online credit card fraud:
    - Use encryption technology
    - Verify the address submitted online against the issuing bank
    - Request a card verification value (CVV)
    - Use transaction-risk scoring software
- Smart cards
    - Contain a memory chip
    - Updated with encrypted data each time card is used
    - Used widely in Europe
    - Not widely used in the U.S.

Hacktivists and Cyberterrorists

- Hacktivism
    - Hacking to achieve a political or social goal
- Cyberterrorist

- Attacks computers or networks in an attempt to intimidate or coerce a government in order to advance certain political or social objectives
- Seeks to cause harm rather than gather information
- Uses techniques that destroy or disrupt services

Federal Laws for Prosecuting Computer Attacks

TABLE 3-5 Federal laws that address computer crime

Federal law	Subject area
USA Patriot Act	Defines cyberterrorism and penalties
Identity Theft and Assumption Deterrence Act (U.S. Code Title 18, Section 1028)	Makes identity theft a Federal crime with penalties up to 15 years imprisonment and a maximum fine of $250,000
Fraud and Related Activity in Connection with Access Devices Statute (U.S. Code Title 18, Section 1029)	False claims regarding unauthorized use of credit cards
Computer Fraud and Abuse Act (U.S. Code Title 18, Section 1030)	Fraud and related activities in association with computers: • Accessing a computer without authorization or exceeding authorized access • Transmitting a program, code, or command that causes harm to a computer • Trafficking of computer passwords • Threatening to cause damage to a protected computer
Stored Wire and Electronic Communications and Transactional Records Access Statutes (U.S. Code Title 18, Chapter 121)	Unlawful access to stored communications to obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage

Source Line: Course Technology/Cengage Learning.

Implementing Trustworthy Computing

- Trustworthy computing
  - Delivers secure, private, and reliable computing
  - Based on sound business practices

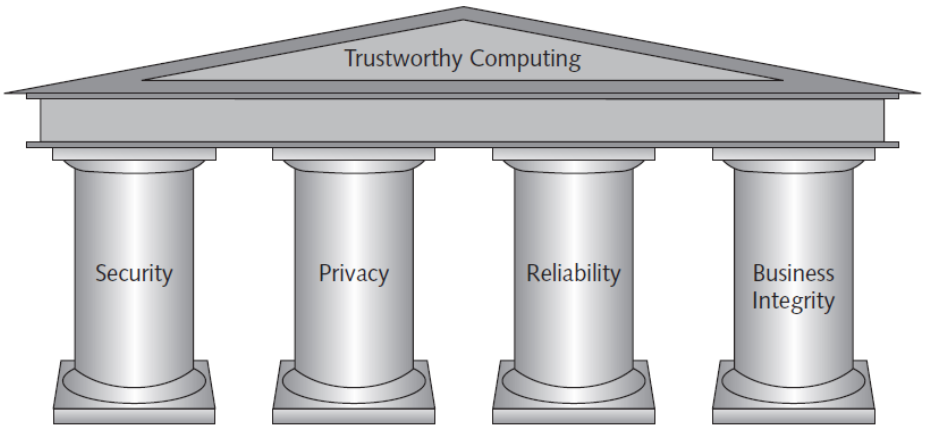

FIGURE 3-4 Microsoft's four pillars of trustworthy computing
Source Line: Course Technology/Cengage Learning.

- Security of any system or network
  - Combination of technology, policy, and people
  - Requires a wide range of activities to be effective
- Systems must be monitored to detect possible intrusion
- Clear reaction plan addresses:
  - Notification, evidence protection, activity log maintenance, containment, eradication, and recovery

Risk Assessment

- Process of assessing security-related risks:
  - To an organization's computers and networks
  - From both internal and external threats
- Identifies investments that best protect from most likely and serious threats
- Focuses security efforts on areas of highest payoff
- Eight-step risk assessment process
  - #1 Identify assets of most concern
  - #2 Identify loss events that could occur
  - #3 Assess likelihood of each potential threat
  - #4 Determine the impact of each threat
  - #5 Determine how each threat could be mitigated
  - #6 Assess feasibility of mitigation options
  - #7 Perform cost-benefit analysis
  - #8 Decide which countermeasures to implement

TABLE 3-7 Risk assessment for hypothetical company

Risk	Business objective threatened	Estimated probability of such an event occurring	Estimated cost of a successful attack	Probability × cost = expected cost	Assessment of current level of protection	Relative priority to be fixed
Distributed denial-of-service attack	24/7 operation of a retail Web site	40%	$500,000	$200,000	Poor	1
Email attachment with harmful worm	Rapid and reliable communications among employees and suppliers	70%	$200,000	$140,000	Poor	2
Harmful virus	Employees' use of personal productivity software	90%	$50,000	$45,000	Good	3
Invoice and payment fraud	Reliable cash flow	10%	$200,000	$20,000	Excellent	4

(Continued)

Source Line: Course Technology/Cengage Learning.

Establishing a Security Policy

- A security policy defines:
  - Organization's security requirements
  - Controls and sanctions needed to meet the requirements
- Delineates responsibilities and expected behavior
- Outlines what needs to be done
  - Not how to do it
- Automated system policies should mirror written policies
- Trade-off between:
  - Ease of use
  - Increased security
- Areas of concern
  - Email attachments
  - Wireless devices

- VPN uses the Internet to relay communications but maintains privacy through security features
- Additional security includes encrypting originating and receiving network addresses

Educating Employees, Contractors, and Part-Time Workers

- Educate and motivate users to understand and follow policy
- Discuss recent security incidents

- Help protect information systems by:
  - Guarding passwords
  - Not allowing sharing of passwords
  - Applying strict access controls to protect data
  - Reporting all unusual activity
  - Protecting portable computing and data storage devices

Prevention

- Implement a layered security solution
  - Make computer break-ins harder
- Installing a corporate firewall
  - Limits network access
- Intrusion prevention systems
  - Block viruses, malformed packets, and other threats
- Installing antivirus software
  - Scans for sequence of bytes or virus signature
  - United States Computer Emergency Readiness Team (US-CERT) serves as clearinghouse

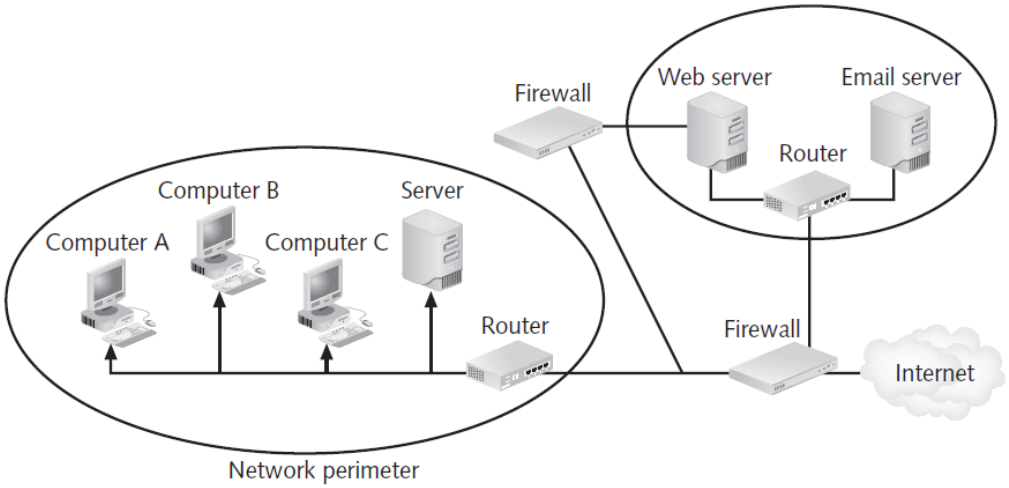

FIGURE 3-6 Firewall
Source Line: Course Technology/Cengage Learning.

TABLE 3-8 Popular firewall software for personal computers

Software	Vendor
Zone Alarm Pro	CheckPoint Software Technologies Ltd.
F-Secure Internet Security	F-Secure Corporation
Panda Global Protection	Panda Security
NeT Firewall	NT Kernel Resources
ESET Smart Security 4	ESET

Source Line: "Best Firewall Software–Editor's Choice," All-Internet-Security.com, © January 2011, www.all-internet-security.com/top_10_firewall_software.html.

- Safeguards against attacks by malicious insiders
- Departing employees and contractors
  - Promptly delete computer accounts, login IDs, and passwords
- Carefully define employee roles and separate key responsibilities
- Create roles and user accounts to limit authority
- Defending against cyberterrorism
  - Department of Homeland Security and its National Cyber Security Division (NCSD) is a resource
    - Builds and maintains a national security cyberspace response system
    - Implements a cyber-risk management program for protection of critical infrastructure, including banking and finance, water, government operations, and emergency services
- Conduct periodic IT security audits
  - Evaluate policies and whether they are followed
  - Review access and levels of authority

- Test system safeguards
- Information Protection Assessment kit is available from the Computer Security Institute

Detection

- Detection systems
  - Catch intruders in the act
- Intrusion detection system
  - Monitors system/network resources and activities
  - Notifies the proper authority when it identifies:
    - Possible intrusions from outside the organization
    - Misuse from within the organization
  - Knowledge-based approach
  - Behavior-based approach

Response

- Response plan
  - Develop well in advance of any incident
  - Approved by:
    - Legal department
    - Senior management
- Primary goals
  - Regain control and limit damage
  - Not to monitor or catch an intruder
- Only 56% have response plan
- Incident notification defines:
  - Who to notify
  - Who not to notify
- Security experts recommend against releasing specific information about a security compromise in public forums
- Document all details of a security incident
  - All system events
  - Specific actions taken
  - All external conversations
- Act quickly to contain an attack
- Eradication effort
  - Collect and log all possible criminal evidence
  - Verify necessary backups are current and complete

    - Create new backups
- Follow-up
    - Determine how security was compromised
        - Prevent it from happening again
- Review
    - Determine exactly what happened
    - Evaluate how the organization responded
- Weigh carefully the amount of effort required to capture the perpetrator
- Consider the potential for negative publicity
- Legal precedent
    - Hold organizations accountable for their own IT security weaknesses

Computer Forensics

- Combines elements of law and computer science to identify, collect, examine, and preserve data and preserve its integrity so it is admissible as evidence
- Computer forensics investigation requires extensive training and certification and knowledge of laws that apply to gathering of criminal evidence

Summary

- Ethical decisions in determining which information systems and data most need protection
- Most common computer exploits
  - Viruses
  - Worms
  - Trojan horses
  - Distributed denial-of-service attacks
  - Rootkits
  - Spam
  - Phishing, spear-fishing, smishing, vishing
- Perpetrators include:
  - Hackers
  - Crackers
  - Malicious insider
  - Industrial spies
  - Cybercriminals
  - Hacktivist
  - Cyberterrorists
- Must implement multilayer process for managing security vulnerabilities, including:
  - Assessment of threats
  - Identifying actions to address vulnerabilities
  - User education
- IT must lead the effort to implement:
  - Security policies and procedures
  - Hardware and software to prevent security breaches
- Computer forensics is key to fighting computer crime in a court of law

Activity

Directions: Identify the following. Write your answer on the space provided.

_____1. “Fix” to a certain program that aims to eliminate the problem.

_____2. Pieces of programming code that is usually disguised as something else that causes unexpected and undesirable behavior to the computer and is often attached to files.

_____3. Harmful programs that resides in the active memory of a computer and duplicate themselves.

_____4. Set of programs that enables its user to gain administrator-level access to a computer without the end user's consent or knowledge.

_____5. Abuse of email systems to send unsolicited email to large numbers of people.

_____6. Act of using email fraudulently to try to get the recipient to reveal personal data.

_____7. People that test the limitations of systems out of intellectual curiosity.

_____8. An act of hacking to achieve a political or social goal.

_____9. People that attacks computers or networks in an attempt to intimidate or coerce a government in order to advance certain political or social objectives.

_____10. The key to fighting computer crime in a court of law.

Chapter 4: Privacy

Objectives

As you read this chapter, consider the following questions:

- What is the right of privacy, and what is the basis for protecting personal privacy under the law?
- What are some of the laws that provide protection for the privacy of personal data, and what are some of the associated ethical issues?
- What is identity theft, and what techniques do identity thieves use?
- What are the various strategies for consumer profiling, and what are the associated ethical issues?
- What must organizations do to treat consumer data responsibly?
- Why and how are employers increasingly using workplace monitoring?
- What are the capabilities of advanced surveillance technologies, and what ethical issues do they raise?

Privacy Protection and the Law

- Systems collect and store key data from every interaction with customers to make better decisions
- Many object to data collection policies of government and business
- Privacy
  - Key concern of Internet users
  - Top reason why nonusers still avoid the Internet
- Reasonable limits must be set
- Historical perspective on the right to privacy
  - Fourth Amendment reasonable expectation of privacy

Information Privacy

- Definition of privacy
  - "The right to be left alone—the most comprehensive of rights, and the right most valued by a free people"
- Information privacy is a combination of:
  - Communications privacy
    - Ability to communicate with others without being monitored by other persons or organizations
  - Data privacy
    - Ability to limit access to one's personal data by other individuals and organizations in order to exercise a substantial degree of control over that data and its use

Privacy Laws, Applications, and Court Rulings

- Legislative acts passed over the past 40 years
  - Most address invasion of privacy by the government
  - No protection of data privacy abuses by corporations
  - No single, overarching national data privacy policy
- Financial data
  - Fair Credit Reporting Act (1970)
    - Regulates operations of credit-reporting bureaus
  - Fair and Accurate Credit Transactions Act (2003)
    - Allows consumers to request and obtain a free credit report once each year from each of the three primary consumer credit reporting companies
  - Right to Financial Privacy Act (1978)
    - Protects the financial records of financial institution customers from unauthorized scrutiny by the federal government
  - Gramm-Leach-Bliley Act (1999)
    - Bank deregulation that enabled institutions to offer investment, commercial banking, and insurance services
    - Three key rules affecting personal privacy
      - Financial Privacy Rule
      - Safeguards Rule
      - Pretexting Rule
- Opt-out policy
  - Assumes that consumers approve of companies collecting and storing their personal information
  - Requires consumers to actively opt out
  - Favored by data collectors

- Opt-in policy
  - Must obtain specific permission from consumers before collecting any data
  - Favored by consumers
- Health information
  - Health Insurance Portability and Accountability Act (1996)
    - Improves the portability and continuity of health insurance coverage
    - Reduces fraud, waste, and abuse
    - Simplifies the administration of health insurance
  - American Recovery and Reinvestment Act (2009)
    - Included strong privacy provisions for electronic health records
    - Offers protection for victims of data breaches
- State laws related to security breach notification
  - Over 40 states have enacted legislation requiring organizations to disclose security breaches
  - For some states, these laws are quite stringent
- Children's personal data
  - Children's Online Privacy Protection Act (1998)
    - Web sites catering to children must offer comprehensive privacy policies, notify parents or guardians about its data-collection practices, and receive parental consent before collecting personal information from children under 13
  - Family Education Rights and Privacy Act (1974)
    - Assigns rights to parents regarding their children's education records
    - Rights transfer to student once student becomes 18
- Electronic surveillance
  - Communications Act of 1934

- Established the Federal Communications Commission
- Regulates all non-federal-government use of radio and television plus all interstate communications

- Title III of the Omnibus Crime Control and Safe Streets Act (Wiretap Act)
  - Regulates interception of telephone and oral communications
  - Has been amended by new laws
  - Foreign Intelligence Surveillance Act (FISA) of 1978
    - Describes procedures for electronic surveillance and collection of foreign intelligence information in communications between foreign powers and agents of foreign powers

- Electronic Communications Privacy Act of 1986 (ECPA)
  - Protects communications in transfer from sender to receiver
  - Protects communications held in electronic storage
  - Prohibits recording dialing, routing, addressing, and signaling information without a search warrant
    - Pen register records electronic impulses to identify numbers dialed for outgoing calls
    - Trap and trace records originating number of incoming calls

- Communications Assistance for Law Enforcement Act (CALEA) 1994
  - Amended both the Wiretap Act and ECPA
  - Required the telecommunications industry to build tools into its products so federal investigators could eavesdrop and intercept electronic communications
  - Covered emerging technologies, such as:
    - Wireless modems
    - Radio-based electronic mail
    - Cellular data networks

- USA PATRIOT Act (2001)
  - Increased ability of law enforcement agencies to search telephone, email, medical, financial, and other records
  - Critics argue law removed many checks and balances that ensured law enforcement did not abuse its powers
  - Relaxed requirements for National Security Letters (NSLs)

- Export of personal data
  - Organization for Economic Co-operation and Development Fair Information Practices (1980)
    - Fair Information Practices
      - Set of eight principles
      - Model of ethical treatment of consumer data
  - European Union Data Protection Directive
    - Requires companies doing business within the borders of 15 European nations to implement a set of privacy directives on the fair and appropriate use of information
    - Goal to ensure data transferred to non-European countries is protected
    - Based on set of seven principles for data privacy
    - Concern that U.S. government can invoke USA PATRIOT Act to access data

- BBBOnLine and TRUSTe
  - Independent initiatives that favor an industry-regulated approach to data privacy
  - BBBOnLine reliability seal or a TRUSTe data privacy seal demonstrates that Web site adheres to high level of data privacy

  - Seals
    - Increase consumer confidence in site

- Help users make more informed decisions about whether to release personal information

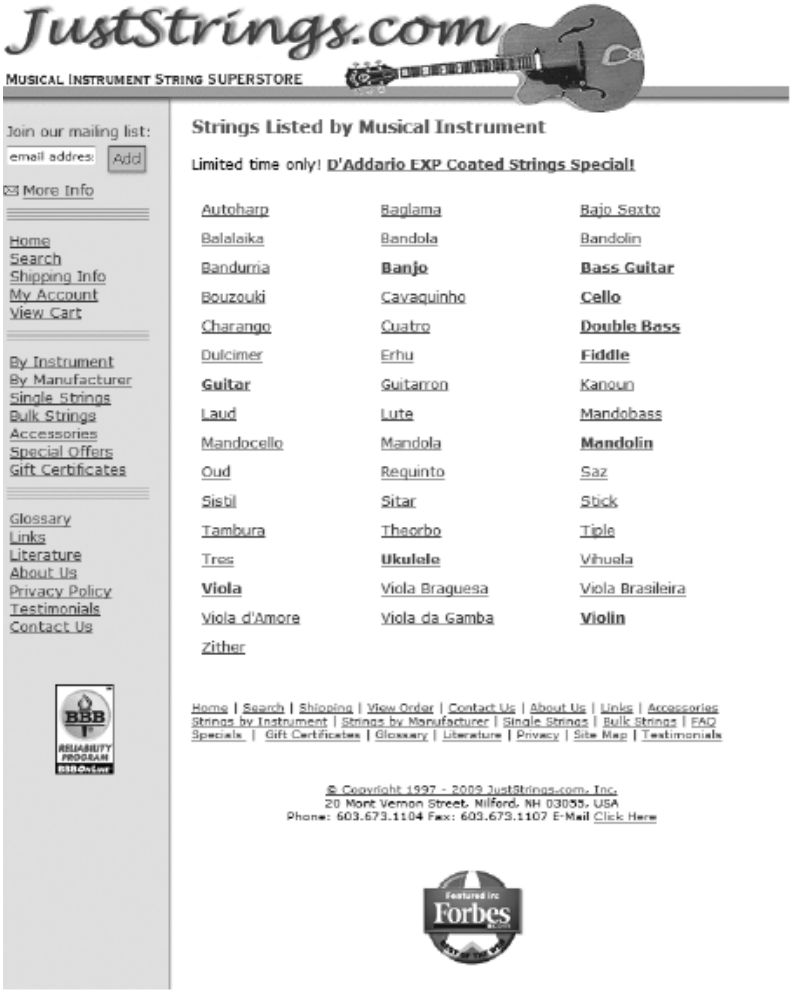

FIGURE 4-1 JustStrings.com displays the BBBOnLine Reliability Program seal
Credit: From www.juststrings.com. Reprinted by permission of JustStrings.com.

- Access to government records
  - Freedom of Information Act (1966 amended 1974)
    - Grants citizens the right to access certain information and records of the federal government upon request
    - Exemptions bar disclosure of information that could:
      - Compromise national security
      - Interfere with active law enforcement investigation

        - Invade someone's privacy

- Access to government records (cont'd.)
    - The Privacy Act of 1974
        - Prohibits government agencies from concealing the existence of any personal data record-keeping system
        - Outlines 12 requirements that each record-keeping agency must meet
        - CIA and law enforcement agencies are excluded from this act
        - Does not cover actions of private industry

Key Privacy and Anonymity Issues

- Identity theft
- Electronic discovery
- Consumer profiling
- Treating customer data responsibly
- Workplace monitoring
- Advanced surveillance technology

Identity Theft

- Theft of key pieces of personal information to impersonate a person, including:
    - Name
    - Address
    - Date of birth
    - Social Security number
    - Passport number

- Driver's license number
- Mother's maiden name

- Fastest-growing form of fraud in the United States
- Consumers and organizations are becoming more vigilant and proactive in fighting identity theft
- Four approaches used by identity thieves
  - Create a data breach
  - Purchase personal data
  - Use phishing to entice users to give up data
  - Install spyware to capture keystrokes of victims
- Data breaches of large databases
  - To gain personal identity information
  - May be caused by:
    - Hackers
    - Failure to follow proper security procedures
- Purchase of personal data
  - Black market for:
    - Credit card numbers in bulk—$.40 each
    - Logon name and PIN for bank account—$10
    - Identity information—including DOB, address, SSN, and telephone number—$1 to $15
- Phishing
  - Stealing personal identity data by tricking users into entering information on a counterfeit Web site
- Spyware
  - Keystroke-logging software

- Enables the capture of:
  - Account usernames
  - Passwords
  - Credit card numbers
  - Other sensitive information
- Operates even if infected computer is not online

- Identity Theft and Assumption Deterrence Act of 1998 was passed to fight fraud
- Identity Theft Monitoring Services
  - Monitor the three major credit reporting agencies (TransUnion, Equifax, and Experian)
  - Monitor additional databases (financial institutions, utilities, and DMV)

Electronic Discovery

- Collection, preparation, review, and production of electronically stored information for use in criminal and civil actions
- Quite likely that information of a private or personal nature will be disclosed during e-discovery
- Federal Rules of Procedure define e-discovery processes
- E-discovery is complicated and requires extensive time to collect, prepare, and review data
- Raises many ethical issues
  - Should an organization attempt to destroy or conceal incriminating evidence?
  - To what degree must an organization be proactive and thorough in providing evidence?
  - Should an organization attempt to “bury” incriminating evidence in a mountain of trivial, routine data?

Consumer Profiling

- Companies openly collect personal information about Internet users
- Cookies
  - Text files that a Web site can download to visitors' hard drives so that it can identify visitors later
- Tracking software analyzes browsing habits
- Similar controversial methods are used outside the Web environment
- Aggregating consumer data
  - Databases contain a huge amount of consumer behavioral data
  - Affiliated Web sites are served by a single advertising network
- Collecting data from Web site visits
  - Goal: provide customized service for each consumer
  - Types of data collected
    - GET data
    - POST data
    - Click-stream data
- Four ways to limit or stop the deposit of cookies on hard drives
  - Set the browser to limit or stop cookies
  - Manually delete them from the hard drive
  - Download and install a cookie-management program
  - Use anonymous browsing programs that don't accept cookies
- Personalization software
  - Used by marketers to optimize the number, frequency, and mixture of their ad placements
    - Rules-based
    - Collaborative filtering

    - Demographic filtering
    - Contextual commerce
- Consumer data privacy
    - Platform for Privacy Preferences (P3P)
        - Shields users from sites that don't provide the level of privacy protection desired

Treating Consumer Data Responsibly

- Strong measures are required to avoid customer relationship problems
- Companies should adopt:
    - Fair Information Practices
    - 1980 OECD privacy guidelines
- Federal Trade Commission responsible for protecting privacy of U.S. consumers
- Chief privacy officer (CPO)
    - Executive to oversee data privacy policies and initiatives

TABLE 4-6 Manager's checklist for treating consumer data responsibly

Question	Yes	No
Does your company have a written data privacy policy that is followed?		
Can consumers easily view your data privacy policy?		
Are consumers given an opportunity to opt in or opt out of your data policy?		
Do you collect only the personal information needed to deliver your product or service?		
Do you ensure that the information is carefully protected and accessible only by those with a need to know?		
Do you provide a process for consumers to review their own data and make corrections?		
Do you inform your customers if you intend to use their information for research or marketing and provide a means for them to opt out?		
Have you identified a person who has full responsibility for implementing your data policy and dealing with consumer data issues?		

Source Line: Course Technology/Cengage Learning.

Workplace Monitoring

- Employers monitor workers
  - Protect against employee abuses that reduce worker productivity or expose employer to harassment lawsuits
- Fourth Amendment cannot be used to limit how a private employer treats its employees
  - Public-sector employees have far greater privacy rights than in the private industry
- Privacy advocates want federal legislation
  - To keep employers from infringing upon privacy rights of employees

Advanced Surveillance Technology

- Camera surveillance
  - Many cities plan to expand surveillance systems
  - Advocates argue people have no expectation of privacy in a public place
  - Critics concerned about potential for abuse
- Global positioning system (GPS) chips
  - Placed in many devices
  - Precisely locate users
  - Banks, retailers, airlines eager to launch new services based on knowledge of consumer location

Summary

- Laws, technical solutions, and privacy policies are required to balance needs of business against rights of consumers
- A number of laws have been enacted that affect a person's privacy particularly in the areas of financial and health records, protection following a security breach, children's personal data, electronic surveillance, export of personal data, and access to government records
- Identity theft is fastest-growing form of fraud
- E-discovery can be expensive, can reveal data of a private or personal data, and raises many ethical issues
- Web sites collect personal data about visitors
- Consumer data privacy has become a major marketing issue
- Code of Fair Information Practices and 1980 OECD privacy guidelines provide an approach to treating consumer data responsibly
- Employers monitor employees to maintain employee productivity and limit exposure to harassment lawsuits
- Advances in information technology provide new data-gathering capabilities but also diminish individual privacy
  - Surveillance cameras
  - GPS systems

Activity

Directions: Choose the most correct answer from the given set.

Right to Financial Privacy Act (1978)	Fair Credit Reporting Act(1970)	Freedom of Information Act(1966 amended 1974)	Gramm-Leach-Bliley Act (1999)	Children's Online Privacy Protection Act (1998)
Privacy Act of 1974	Communications Act of 1934	Fair and Accurate Credit Transactions Act (2003)	Opt-in policy	Opt-out policy

_____1. Allows consumers to request and obtain a free credit report once each year from each of the three primary consumer credit reporting companies.

_____2. It assumes that consumers approve of companies collecting and storing their personal information.

_____3. States that companies must obtain specific permission from consumers before collecting any data.

_____4. Protects the financial records of financial institution customers from unauthorized scrutiny by the federal government.

_____5. Grants citizens the right to access certain information and records of the federal government upon request.

_____6. Web sites catering to children must offer comprehensive privacy policies, notify parents or guardians about its data-collection practices, and receive parental consent before collecting personal information from children under 13.

_____7. Established the Federal Communications Commission that regulates all non-federal-government use of radio and television plus all interstate communications.

_____8. Bank deregulation that enabled institutions to offer investment, commercial banking, and insurance services.

_____9. Regulates operations of credit-reporting bureaus.

_____10. Prohibits government agencies from concealing the existence of an

Chapter 5: Freedom of Expression

Objectives

As you read this chapter, consider the following questions:

- What is the basis for the protection of freedom of expression in the United States, and what types of expression are not protected under the law?
- What are some key federal laws that affect online freedom of expression, and how do they impact organizations?
- What important freedom of expression issues relate to the use of information technology?

First Amendment Rights

- Right to freedom of expression
  - Important right for free people everywhere
  - Guaranteed by the First Amendment
- Definition of free speech includes:
  - Nonverbal, visual, and symbolic forms of expression
  - Right to speak anonymously
- Not protected by the First Amendment
  - Perjury
  - Fraud
  - Defamation
  - Obscene speech
  - Incitement of panic
  - Incitement to crime
  - “Fighting words”
  - Sedition

Perjury

- Also known as forswearing
  - Willful act of swearing a false oath

A crime that occurs when an individual willfully makes a false statement during a judicial proceeding, after he or she has taken an oath to speak the truth.

Fraud

The crime of using dishonest methods to take something valuable from another person. A person who pretends to be what he or she is not in order to trick.

Defamation

the action of damaging the good reputation of someone; slander or libel.

- Oral or written statement of alleged fact that is:
  - False
  - Harms another person
    - Harm is often of a financial nature
- Slander
  - Oral defamatory statement
- Libel
  - Written defamatory statement

Sedition

The crime of saying, writing, or doing something that encourages people to disobey their government

Obscene Speech

- Based on Miller v. California, speech is considered obscene when:
  - Average person finds the work appeals to the prurient interest
    - Prurient - having or encouraging an excessive interest in sexual matters.
  - Work depicts or describes sexual conduct in an offensive way
  - Lacks serious literary, artistic, political, or scientific value

Incitement of Panic

Inducing **panic** is when a person causes the evacuation of any public place, or otherwise cause serious public inconvenience or alarm.

Incitement of Crime

the plan to commit **crime** may exist only in the mind of one person until others are **incited** to join in, at which point the social danger becomes more real.

Fighting words

Are generally words so offensive that it makes a person angry. These words often precede a physical or verbal fight or argument. What constitutes a fighting word can vary from person to person. Not everyone will have the same words on their list. What makes one person angry may not bother another. Some fighting words that commonly invoke strong feelings are those that insult a family member, particularly one's mother. Calling someone a liar, cheater, or stupid can also cause arguments or fights to arise.

Freedom of Expression: Key Issues

- Controlling access to information on the Internet
- Anonymity on the Internet
- Defamation and hate speech
- Corporate blogging
- Pornography

Controlling Access to Information on the Internet

- Freedom of speech on the Internet is complicated by ease by which children can access Internet
- Communications Decency Act (CDA)
  - Aimed at protecting children from pornography
  - Broad language and vague definition of indecency
  - Found unconstitutional in 1997
- Child Online Protection Act (COPA)
  - Applies to communication for commercial purposes
  - Imposes penalties for exposing minors to harmful material on the Web
  - Found unconstitutional in 2004
- Internet filtering
  - Software installed with a Web browser

    - Blocks access to certain Web sites deemed to contain inappropriate or offensive material
- URL filtering
    - Blocks objectionable URLs or domain names
- Keyword filtering
    - Blocks keywords or phrases
- Dynamic content filtering
    - Web site's content is evaluated immediately before being displayed
    - Uses
        - Object analysis
        - Image recognition
- Top-rated Internet filters for home users
    - NetNanny Parental Controls
    - PureSight PC
    - CYBERsitter
    - SafeEyes
    - CyberPatrol
- ICRA rating system
    - Questionnaire for Web authors
    - Generates a content label
        - Platform for Internet Content Selection (PICS)
    - Users configure browsers to read the label
    - Relies on Web authors to rate their site
    - Complement to other filtering techniques
- ISP blocking
    - Blocking is performed on the ISP server
    - ClearSail/Family.NET prevents access to certain Web sites

Children's Internet Protection Act (CIPA)

- Federally financed schools and libraries must block computer access to:
    - Obscene material
    - Pornography
    - Anything considered harmful to minors
- Schools and libraries subject to CIPA do not receive Internet access discounts unless they:
    - Put in place measures to filter pictures that are obscene, contain child pornography, or are harmful to minors
    - Adopt a policy to monitor the online activities of minors
    - Adopt a policy restricting minors' access to materials harmful to them

- CIPA does not require the tracking of Internet use by minors or adults
- Acceptable use policy agreement is an essential element of a successful program in schools
  - Signed by:
    - Students
    - Parents
    - Employees
- Difficulty implementing CIPA in libraries because their services are open to people of all ages
  - Including adults with First Amendment rights
- CIPA has been upheld as constitutional by U.S. Supreme Court (U.S. v American Library Association)

Anonymity on the Internet

- Anonymous expression is expression of opinions by people who do not reveal their identity
- Freedom to express an opinion without fear of reprisal is an important right in democratic society
- Anonymity is even more important in countries that do not allow free speech
- Played important role in early formation of U.S.
- In the wrong hands, it can be a tool to commit illegal or unethical activities
- Anonymous remailer service
  - Computer program that strips the originating address from the email message
  - Forwards the message to the intended recipient
  - Ensures no header information can identify the author
  - Keeps what is communicated anonymous
  - What is communicated and whether it is ethical or unethical, legal or illegal, is up to the sender
- John Doe lawsuit
  - Defendant communicates using a pseudonym or anonymously so identity of defendant is temporarily unknown
  - Common in Internet libel cases
  - Once John Doe lawsuit is filed, the company may request court permission to issue subpoenas
  - ISPs frequently subpoenaed to provide the identity of anonymous “John Does”
  - Anonymity on the Internet cannot be guaranteed

Defamation and Hate Speech

- Hate speech that can be prosecuted includes:
  - Clear threats and intimidation against specific citizens
  - Sending threatening private messages over the Internet to a person
  - Displaying public messages on a Web site describing intent to commit acts of hate-motivated violence against specific individuals
  - Libel directed at a particular person
- Many ISPs reserve right to remove content that does not meet their standards
- Such actions do not violate the subscriber's First Amendment rights because these prohibitions are in the terms of service
  - ISPs must monitor the use of their service
  - Take action when terms are violated
- Public schools and universities are legally considered agents of the government and must follow the First Amendment prohibition against speech restrictions
- Corporations, private schools, and private universities not part of state or federal government
  - May prohibit students, instructors, and employees from engaging in offensive speech

Corporate Blogging

- Some organizations allow employees to create their own personal blogs to:
  - Reach out to partners, customers, and employees
  - Improve their corporate image
- Blogs can provide uncensored commentary and interaction
  - Criticism of corporate policies and decisions
- Could involve risk that employees might:
  - Reveal company secrets
  - Breach federal security disclosure laws

Pornography

- The Internet has been a boon *(a thing that is helpful or beneficial)*. to the pornography industry
  - More than 4.2 million porn Web sites are accessible
  - The sites generate an estimated $1 to $7 billion a year in revenue
  - 72 million estimated visitors to porn Web sites monthly

- Individuals free to produce and publish what they want; however, if what they distribute is judged obscene, they are subject to prosecute
  - *California v Miller* set precedent for what is obscene
- Many organizations take steps to stop access in the workplace
  - Establishing a computer usage policy that prohibits access to pornography sites
  - Identifying those who violate the policy
  - Taking action against those users
  - Failure to take action against pornography could result in sexual harassment lawsuit
- Numerous federal laws address child pornography
  - Federal offense to produce or distribute
  - Most states outlaw possession as well
- At least seven states require computer technicians to report child pornography on clients' computers
- Sexting is sending of sexual messages, nude or seminude photos, or sexually explicit videos over a cell phone
  - Fast-growing trend
- CAN-SPAM Act
  - Specifies requirements that commercial retailers must follow when sending messages
  - Each violation can result in $250 - $750 fine
  - Federal Trade Commission charged with enforcing the act, but has not done so effectively
  - Deterrent in fighting the dissemination of pornography

Summary

- First Amendment protects the right to:
  - Freedom of religion and expression
- Does not protect obscene speech, defamation
- Key issues
  - Controlling access to Internet information, especially for children
  - Anonymous communication
  - Spread of defamation and hate speech
  - Access to pornography
  - CAN-SPAM Act limitations on email messages

Activity

Enumeration

1. Offenses not protected by the First Amendment.

_____ _____

_____ _____

_____ _____

_____ _____

2. Types of Defamation

_____

_____

3. Key Issues of the Freedom of Expression

_____

_____

_____

_____

_____

4. Top-rated Internet filters for home users

_____

_____

_____

_____

Chapter 6: Intellectual Property

Objectives

As you read this chapter, consider the following questions:

- What does the term intellectual property encompass, and why are organizations so concerned about protecting intellectual property?
- What are the strengths and limitations of using copyrights, patents, and trade secret laws to protect intellectual property?
- What is plagiarism, and what can be done to combat it?
- What is reverse engineering, and what issues are associated with applying it to create a look-alike of a competitor's software program?
- What is open source code, and what is the fundamental premise behind its use?
- What is the essential difference between competitive intelligence and industrial espionage, and how is competitive intelligence gathered?
- What is cybersquatting, and what strategy should be used to protect an organization from it?

What Is Intellectual Property?

- Term used to describe works of the mind
  - Distinct and "owned" or created by a person or group
- Copyright law
  - Protects authored works
- Patent law
  - Protects inventions
- Trade secret law
  - Helps safeguard information critical to an organization's success

Copyrights

- Established in the U.S. Constitution
  - Article I, Section 8, Clause 8

- Grants creators of original works the exclusive right to:
  - Distribute
  - Display
  - Perform
  - Reproduce work
  - Prepare derivative works based upon the work
- Author may grant exclusive right to others
- Copyright term
  - Copyright law guarantees developers the rights to their works for a certain amount of time
- Sonny Bono Copyright Term Extension Act
  - Created after 1/1/78, life of the author plus 70 years
  - Created but not published or registered before 1/1/78, life of the author plus 70 years; no expiration before 12/31/2004
  - Created before 1978 still in original or renewable term of copyright, 95 years from the date the copyright was originally secured
- Types of work that can be copyrighted
  - Architecture
  - Art
  - Audiovisual works
  - Choreography
  - Drama
  - Graphics
  - Literature
  - Motion pictures
- Types of work that can be copyrighted (cont'd.)
  - Music
  - Pantomimes
  - Pictures
  - Sculptures
  - Sound recordings
  - Other intellectual works:
    - As described in Title 17 of U.S. Code
- Must fall within one of the preceding categories
- Must be original
  - Evaluating originality can cause problems
- Fair use doctrine
  - Allows portions of copyrighted materials to be used without permission under certain circumstances

    - Maintains balance between protecting an author's rights and enabling public access to copyrighted works
    - Factors to consider when evaluating the use of copyrighted material
- Fair use doctrine factors include:
    - Purpose and character of the use
    - Nature of the copyrighted work
    - Portion of the copyrighted work used
    - Effect of the use upon the value of the copyrighted work
    - Key concept: an idea cannot be copyrighted, but the expression of an idea can be
- Copyright infringement
    - Copy substantial and material part of another's copyrighted work
    - Without permission
- Software copyright protection
    - Raises many complicated issues of interpretation
    - Copyright law should not be used to inhibit interoperability between the products of rival vendors
- The Prioritizing Resources and Organization for Intellectual Property (PRO-IP) Act of 2008
    - Increased enforcement and substantially increased penalties for infringement
- General Agreement on Tariffs and Trade (GATT)
    - Trade agreement between 117 countries
    - Created World Trade Organization (WTO) to enforce
    - Despite GATT, copyright protection varies greatly from country to country
- The WTO and the WTO TRIPS Agreement (1994) (Trade-Related Aspects of Intellectual Property Rights)
    - Many nations recognize that intellectual property has become increasingly important in world trade
    - Established minimum levels of protection that each government must provide to the intellectual property of members
    - Covers copyright, patents, and trade secrets
- World Intellectual Property Organization (WIPO)
    - Agency of the United Nations
    - Advocates for the interests of intellectual property owners
    - WIPO Copyright Treaty provides additional copyright protections for electronic media

TABLE 6-1 Summary of the WTO TRIPS Agreement

Form of intellectual property	Key terms of agreement
Copyright	Computer programs are protected as literary works. Authors of computer programs and producers of sound recordings have the right to prohibit the commercial rental of their works to the public.
Patent	Patent protection is available for any invention—whether a product or process—in all fields of technology without discrimination, subject to the normal tests of novelty, inventiveness, and industrial applicability. It is also required that patents be available and patent rights enjoyable without discrimination as to the place of invention and whether products are imported or locally produced.
Trade secret	Trade secrets and other types of undisclosed information that have commercial value must be protected against breach of confidence and other acts that are contrary to honest commercial practices. However, reasonable steps must have been taken to keep the information secret.

Source Line: World Trade Organization, "Overview: The TRIPS Agreement," *www.wto.org/english/tratop_e/trips_e/intel2_e.htm*.

- Digital Millennium Copyright Act (DMCA)
  - Civil and criminal penalties included
  - Governs distribution of tools and software that can be used to circumvent technological measures used to protect copyrighted works
  - Provides safe harbors for ISPs whose customers/subscribers may be breaking copyright laws
    - ISP must comply with "notice and takedown procedures" that grant copyright holders a process to halt access to alleged infringing content

Patents

- Grant of property right to inventors
- Issued by the U.S. Patent and Trademark Office (USPTO)
- Permits an owner to exclude the public from making, using, or selling the protected invention
- Allows legal action against violators
- Prevents independent creation as well as copying
- Extends only to the United States and its territories and possessions
- Applicant must file with the USPTO
  - USPTO searches prior art
  - Takes an average of 35.3 months from filing an application until application is issued as a patent or abandoned
- Prior art
  - Existing body of knowledge
  - Available to a person of ordinary skill in the art

- An invention must pass four tests
  - Must be in one of the five statutory classes of items
  - Must be useful
  - Must be novel
  - Must not be obvious to a person having ordinary skill in the same field
- Items cannot be patented if they are:
  - Abstract ideas
  - Laws of nature
  - Natural phenomena
- Patent infringement
  - Making unauthorized use of another's patent
  - No specified limit to the monetary penalty
- Software patent
  - Protects feature, function, or process embodied in instructions executed on a computer
- 20,000 software-related patents per year have been issued since the early 1980s
- Some experts think the number of software patents being granted inhibits new software development
- Before obtaining a software patent, do a patent search
- Software Patent Institute is building a database of information
- Software cross-licensing agreements
  - Large software companies agree not to sue each other over patent infringements
  - Small businesses have no choice but to license patents if they use them
- Average patent lawsuit costs $3 - $10 million
- Defensive publishing
  - Alternative to filing for patents
  - Company publishes a description of the innovation
  - Establishes the idea's legal existence as prior art
  - Costs mere hundreds of dollars
  - No lawyers
  - Fast
- Patent troll firm
  - Acquires patents with no intention of manufacturing anything; instead, licensing the patents to others

- Standard is a definition or format
  - Approved by recognized standards organization or accepted as a de facto standard by the industry
  - Enables hardware and software from different manufacturers to work together
- Submarine patent
  - Patented process/invention hidden within a standard
  - Does not surface until standard is broadly adopted
- Patent farming involves:
  - Influencing a standards organization to make use of a patented item without revealing the existence of the patent
  - Demanding royalties from all parties that use the standard

Trade Secrets

- Trade secret
  - Business information
  - Represents something of economic value
  - Requires an effort or cost to develop
  - Some degree of uniqueness or novelty
  - Generally unknown to the public
  - Kept confidential
- Information is only considered a trade secret if the company takes steps to protect it
- Trade secret law has a few key advantages over patents and copyrights
  - No time limitations
  - No need to file an application
  - Patents can be ruled invalid by courts
  - No filing or application fees
- Law doesn't prevent someone from using the same idea if it is developed independently
- Trade secret law varies greatly from country to country
- Uniform Trade Secrets Act (UTSA)
  - Established uniformity across the states in area of trade secret law
  - Computer hardware and software can qualify for trade secret protection
- The Economic Espionage Act (EEA) of 1996
  - Penalties of up to $10 million and 15 years in prison for the theft of trade secrets

Employees and Trade Secrets

- Employees are the greatest threat to trade secrets
- Unauthorized use of an employer's customer list
  - Customer list is not automatically considered a trade secret
  - Educate workers about the confidentiality of lists
- Nondisclosure clauses in employee's contract
  - Enforcement can be difficult
  - Confidentiality issues are reviewed at the exit interview
- Non-compete agreements
  - Prohibits an employee from working for any competitors for a period of time
  - Protect intellectual property from being used by competitors when key employees leave
  - Require employees not to work for competitors for a period of time
  - Wide range of treatment on non-compete agreements among the various states

Key Intellectual Property Issues

Issues that apply to intellectual property and information technology

- Plagiarism
- Reverse engineering
- Open source code
- Competitive intelligence
- Trademark infringement
- Cybersquatting

Plagiarism

- Stealing someone's ideas or words and passing them off as one's own
- Many students:
  - Do not understand what constitutes plagiarism
  - Believe that all electronic content is in the public domain
- Plagiarism is also common outside academia
- Plagiarism detection systems
  - Check submitted material against databases of electronic content

TABLE 6-3 Partial list of plagiarism detection services and software

Name of service	Web site	Provider
iThenticate	www.ithenticate.com	iParadigms
Turnitin	www.turnitin.com	iParadigms
SafeAssign	www.safeassign.com	Blackboard
Glatt Plagiarism Services	www.plagiarism.com	Glatt Plagiarism Services
EVE Plagiarism Detection	www.canexus.com/eve	CaNexus

Source Line: Course Technology/Cengage Learning.

- Steps to combat student plagiarism
  - Help students understand what constitutes plagiarism and why they need to cite sources
  - Show students how to document Web pages
  - Schedule major writing assignments in portions due over the course of the term
  - Tell students that instructors are aware of Internet paper mills and plagiarism detection services
  - Incorporate detection into an antiplagiarism program

Reverse Engineering

- Process of taking something apart in order to:
  - Understand it
  - Build a copy of it
  - Improve it
- Applied to computer:
  - Hardware
  - Software
- Convert a program code to a higher-level design
- Convert an application that ran on one vendor's database to run on another's
- Compiler
  - Language translator
  - Converts computer program statements expressed in a source language to machine language
- Software manufacturer
  - Provides software in machine language form

- Decompiler
  - Reads machine language
  - Produces source code
- Courts have ruled in favor of reverse engineering:
  - To enable interoperability
- Software license agreements forbid reverse engineering
- Ethics of using reverse engineering are debated
  - Fair use if it provides useful function/interoperability
  - Can uncover designs that someone else has developed at great cost and taken care to protect

Open Source Code

- Program source code made available for use or modification:
  - As users or other developers see fit
- Basic premise
  - Many programmers can help software improve
  - Can be adapted to meet new needs
  - Bugs rapidly identified and fixed
  - High reliability
- GNU General Public License (GPL) was a precursor to the Open Source Initiative (OSI)

Competitive Intelligence

- Gathering of legally obtainable information
  - To help a company gain an advantage over rivals
- Often integrated into a company's strategic plans and decision making
- Not the same as industrial espionage, which uses illegal means to obtain business information not available to the general public
- Without proper management safeguards, it can cross over to industrial espionage

TABLE 6-5 A manager's checklist for running an ethical competitive intelligence operation

Question	Yes	No
Has the competitive intelligence organization developed a mission statement, objectives, goals, and a code of ethics?		
Has the company's legal department approved the mission statement, objectives, goals, and code of ethics?		
Do analysts understand the need to abide by their organization's code of ethics and corporate policies?		
Is there a rigorous training and certification process for analysts?		
Do analysts understand all applicable laws—domestic and international—including the Uniform Trade Secrets Act and the Economic Espionage Act, and do they understand the critical importance of abiding by them?		
Do analysts disclose their true identity as well as the name of their organization prior to any interviews?		

(*Continued*)

TABLE 6-5 A manager's checklist for running an ethical competitive intelligence operation *(Continued)*

Question	Yes	No
Do analysts understand that everything their firm learns about the competition must be obtained legally?		
Do analysts respect all requests for anonymity and confidentiality of information?		
Has the company's legal department approved the processes for gathering data?		
Do analysts provide honest recommendations and conclusions?		
Is the use of third parties to gather competitive intelligence carefully reviewed and managed?		

Source Line: Course Technology/Cengage Learning.

Trademark Infringement

- Trademark is logo, package design, phrase, sound, or word that enables consumer to differentiate one company's product from another's
- Trademark owner can prevent others from using the same mark or a confusingly similar mark on a product's label
- Organizations frequently sue one another over the use of a trademark in a Web site or domain name
- Nominative fair use is defense often employed by defendant in trademark infringement case

Cybersquatting

- Cyber squatters
  - Register domain names for famous trademarks or company names
  - Hope the trademark's owner will buy the domain name for a large sum of money
- To curb cybersquatting, register all possible domain names
  - .org, .com, .info
- Internet Corporation for Assigned Names and Numbers (ICANN)
  - Several top-level domains (.com, .edu, edu., .gov, .int, .mil, .net, .org, aero, .biz, .coop, .info, .museum, .name, .pro, .asis, .cat, .mobi, .tel, and .travel)
  - Current trademark holders are given time to assert their rights in the new top-level domains before registrations are opened to the general public
  - Anti-cybersquatting Consumer Protection Act allows trademark owners to challenge foreign cyber squatters

Summary

- Intellectual property is protected by laws for:
  - Copyrights
  - Patents
  - Trademarks
  - Trade secrets
- Plagiarism is stealing and passing off the ideas and words of another as one's own
- Reverse engineering
  - Process of breaking something down in order to understand, build a copy of, or improve it
- Open source code
  - Made available for use or modification as users or other developers see fit
- Competitive intelligence
  - Uses legal means and public information
- Trademark infringement
  - Use of other's trademark in a Web site can lead to issues
- Cybersquatting
  - Registration of a domain name by an unaffiliated party

Activity

Directions: Answer the following questions with True or False before the number.

_____1. Copyright law protects inventions and Patent law protects authored works.

_____2. Copyright law guarantees developers the rights to their works for a certain amount of time

_____3. Fair use doctrine allows portions of copyrighted materials to be used without permission under certain circumstances

_____4. Patents grants property right to authors.

_____5. An invention must pass three tests before being patented.

_____6. Items cannot be patented if they are Laws of nature

_____7. Software patent protects feature, function, or process embodied in instructions executed on a computer.

_____8. Plagiarism is stealing someone's ideas or words and passing them off as one's own

_____9. A Compiler converts computer program statements expressed in a source language to machine language.

_____10. Trademark is logo, package design, phrase, sound, or word that enables consumer to differentiate one company's product from another's

Chapter 7: Software Quality Development

Objectives

As you read this chapter, consider the following questions:

- Why do companies require high-quality software in business systems, industrial process control systems, and consumer products?
- What potential ethical issues do software manufacturers face in making trade-offs between project schedules, project costs, and software quality?
- What are the four most common types of software product liability claims?
- What are the essential components of a software development methodology, and what are the benefits of using such a methodology?
- How can the Capability Maturity Model Integration improve an organization's software development process?
- What is a safety-critical system, and what special actions are required during its development?

Strategies for Engineering Quality Software

- High-quality software systems:
  - Perform quickly and efficiently
  - Operate safely and reliably
  - Meet their users' needs
  - Are required to support the fields of:
    - Air traffic control
    - Nuclear power
    - Automobile safety
    - Health care
    - Military and defense
    - Space exploration
- Increased demand for high-quality software
- Software defect
  - Could cause a system to fail to meet users' needs
  - Impact may be trivial or very serious
  - Subtle and undetectable or glaringly obvious
- Software quality
  - Degree to which software meets the needs of users
- Quality management
  - Defines, measures, and refines the quality of the development process and products developed
  - Objective
    - Help developers deliver high-quality systems that meet the needs of users
- Deliverables are products such as:
  - Statements of requirements
  - Flowcharts
  - User documentation
- Primary cause for poor software quality:
  - Many developers do not know how to design quality into software from the start
  - Or do not take the time to do so
- Developers must:
  - Define and follow rigorous engineering principles
  - Learn from past mistakes
  - Understand systems' operating environment
  - Design systems relatively immune to human error

- Programmers make mistakes in turning design specifications into code
  - About one defect for every 7-10 lines of code
- Extreme pressure to reduce time to market
  - Driven by need to:
    - Deliver new functionality
    - Begin generating revenue to recover costs
    - Meet quarterly earnings forecasts
  - Resources and time to ensure quality are often cut
- Ethical dilemma: how much additional cost and effort should be expended to ensure products and services meet customers' expectations?
- First release of software
  - Organizations avoid buying the first release
  - Or prohibit its use in critical systems
  - Usually has many defects
- Established software products can also falter:
  - When operating conditions change

The Importance of Software Quality

- Business information systems
  - Set of interrelated components including:
    - Hardware
    - Software
    - Databases
    - Networks
    - People
    - Procedures
  - Collect and process data and disseminate the output
- Business information system examples
  - Manufacturer's order-processing system
  - Bank's electronic-funds transfer system
  - Airline's online ticket reservation system
- Decision support system (DSS)
  - Used to improve decision making
- Software is used to control industrial processes
- Software controls the operation of many industrial and consumer products

- Mismanaged software can be fatal to a business
- Ethical questions
  - How much effort and money to invest to ensure high-quality software
  - Whether products could cause damage and what the legal exposure would be if they did

Software Product Liability

- Product liability
  - Liability of manufacturers, sellers, lessors, and others for injuries caused by defective products
  - There is no federal product liability law
    - Mainly state law
    - Article 2 of the Uniform Commercial Code
- Strict liability
  - Defendant held responsible for the injury
  - Regardless of negligence or intent
- Strict liability
  - Plaintiff must prove only that the software product is defective or unreasonably dangerous and that the defect caused the injury
  - No requirement to prove that the manufacturer was careless or negligent or to prove who caused the defect
  - All parties in the chain of distribution are liable
    - Manufacturer
    - Subcontractors
    - Distributors

- Legal defenses used against strict liability
  - Doctrine of supervening event
  - Government contractor defense
  - Expired statute of limitations
- Negligence
  - Failure to do what a reasonable person would do, or doing something that a reasonable person would not do
  - Responsibility is limited to defects that could have been detected and corrected through “reasonable” software development practices
- Negligence
  - Area of great risk for software manufacturers
  - Defense of negligence may include:

    - Legal justification for the alleged misconduct
    - Demonstration that the plaintiffs' own actions contributed to injuries (contributory negligence)
- Warranty
  - Assures buyers or lessees that a product meets certain standards of quality
  - May be expressly stated or implied by law
- Breach of warranty claim
  - When the product fails to meet the terms of its warranty
  - Plaintiff must have a valid contract that the supplier did not fulfill
  - Can be extremely difficult to prove because the software supplier writes the warranty to limit liability
- Intentional misrepresentation
  - Seller or lessor either misrepresents the quality of a product or conceals a defect in it
  - Forms of representation
    - Advertising
    - Salespersons' comments
    - Invoices
    - Shipping labels

Software Development Process

- Large software project roles
  - System analysts
  - Programmers
  - Architects
  - Database specialists
  - Project managers
  - Documentation specialists
  - Trainers
  - Testers
- Software development methodology
  - Standard, proven work process
  - Controlled and orderly progress
  - Defines activities in software development process
  - Defines individual and group responsibilities
  - Recommends specific techniques for activities
  - Offers guidelines for managing the quality of software during various stages of development

- Easier and cheaper to avoid software problems at the beginning than to attempt to fix damages after the fact
  - Cost to identify and remove a defect in an early stage can be up to 100 times less than removing a defect in distributed software
  - Identify and remove errors early in the development process
    - Cost-saving measure
    - Most efficient way to improve software quality
- Effective methodology protects from legal liability
  - Reduces the number of software errors
  - If an organization follows widely accepted development methods, negligence on its part is harder to prove
- Software quality assurance (QA) refers to methods within the development cycle
  - Guarantee reliable operation of product
  - Are applied at each stage in the development cycle
  - Include testing before the product ships
- Dynamic testing
  - Black-box testing
    - Tester has no knowledge of code
  - White-box testing
    - Testing all possible logic paths in the software unit, with thorough knowledge of the logic
    - Makes each program statement execute at least once
- Static testing
  - Static analyzers are run against the new code
  - Looks for suspicious patterns in programs that might indicate a defect
- Integration testing
  - Occurs after successful unit testing
  - Software units are combined into an integrated subsystem
  - Ensures that all linkages among various subsystems work successfully
- System testing
  - Occurs after successful integration testing
  - Various subsystems are combined
  - Tests the entire system as a complete entity
- User acceptance testing
  - Independent testing performed by trained end users
  - Ensures that the system operates as they expect

- **Capability Maturity Model Integration**
  Process improvement approach
- Defined by the Software Engineering Institute

  - At Carnegie Mellon University in Pittsburgh
- Defines essential elements of effective processes
- General enough to evaluate and improve almost any process
- Frequently used to assess software development practices
- Defines five levels of software development maturity
- Identifies issues most critical to software quality and process improvement
- Organization conducts an assessment of its software development practices
  - Determines where they fit in the capability model
  - Identifies areas for improvement
    - Action plans defined to upgrade the development process
- Maturity level increases
  - Organization improves its ability to deliver good software on time and on budget
- CMMI-Development
  - Set of guidelines for 22 process areas related to systems development
  - Organizations that do these 22 things well will have an outstanding software development and maintenance process

TABLE 7-1 Definition of CMMI maturity levels

Maturity level	Description
Initial	Process is ad hoc and chaotic; organization tends to over commit and processes are often abandoned during times of crisis
Managed	Projects employ processes and skilled people; status of work products is visible to management at defined points
Defined	Processes are well defined and understood and are described in standards, procedures, tools, and methods; processes are consistent across the organization
Quantitatively managed	Quantitative objectives for quality and process performance are established and are used as criteria in managing projects; specific measures of process performance are collected and statistically analyzed
Optimizing	Organization continually improves its processes based on a quantitative understanding of its business objectives and performance needs

Source Line: Used with permission from Carnegie Mellon University.

Key Issues in Software Development

- Consequences of software defects in certain systems can be deadly
  - Companies must take special precautions
- Ethical decisions involve a trade-off between quality and cost, ease of use, and time to market

Development of Safety-Critical Systems

- Safety-critical system
  - A system whose failure may cause injury or death
  - Examples
    - Automobile's antilock brakes
    - Nuclear power plant reactors
    - Airplane navigation
    - Roller coasters
    - Elevators
    - Medical devices
- Key assumption
  - Safety will not automatically result from following the organization's standard development methodology
- Requires a more rigorous and time-consuming development process than other kinds of software
- All tasks require:
  - Additional steps
  - More thorough documentation
  - Vigilant checking and rechecking
- Project safety engineer
  - Explicit responsibility for the system's safety
  - Uses a logging and monitoring system:
    - To track hazards from the project's start to finish
- Hazard log
  - Used at each stage of the software development process to assess how project team has accounted for detected hazards
- Safety reviews
  - Held throughout the development process
- Robust configuration management system
  - Tracks all safety-related documentation
- Formal documentation required
  - Including verification reviews and signatures
- Key issues
  - Ethical dilemmas re: increased time and expense
  - Deciding when QA staff has performed enough testing
- Risk
  - Probability of an undesirable event occurring times the magnitude of the event's consequences
  - Consequences include:
    - Damage to property
    - Loss of money

    - Injury to people
    - Death
- Redundancy
  - Provision of multiple interchangeable components to perform a single function
  - Used to cope with failures and errors
  - During times of widespread disaster, lack of sufficient redundant can lead to major problems
- N-version programming
  - Form of redundancy
  - Involves the execution of a series of program instructions simultaneously by two different systems
  - Uses different algorithms to execute instructions that accomplish the same result
  - Results from the two systems are compared
  - If a difference is found, another algorithm is executed to determine which system yielded the correct result

  - Instructions for the two systems can be:
    - Written by programmers from two different companies
    - Run on different hardware devices
  - Rationale
    - Both systems are highly unlikely to fail at the same time under the same conditions
- Decide what level of risk is acceptable
  - Difficult and controversial decision
  - Make system modifications if level of risk is judged to be too great
- Mitigate the consequences of failure
  - Devise emergency procedures and evacuation plans
- Decide whether to recall a product:
  - When data indicates a problem
- Reliability
  - Probability of a component or system performing without failure over its product life
- Human interface
  - Important and difficult area of safety-critical system design
  - Should leave the operator little room for erroneous judgment
  - Poor design of a system interface can greatly increase risk

Quality Management Standards

- ISO 9001 family of standards
  - Guide to quality products, services, and management
  - Organization must submit to an examination by an external assessor
  - Requirements
    - Written procedures for everything it does
    - Follow those procedures
    - Prove to the auditor the organization fulfilled the first two requirements
- Failure mode and effects analysis (FMEA)
  - Technique used to evaluate reliability and determine the effect of system and equipment failures
  - Failures are classified by:
    - Impact on a project's success
    - Personnel safety
    - Equipment safety
    - Customer satisfaction and safety
  - Goal
    - Identify potential design and process failures early in a project

TABLE 7-4 Manager's checklist for improving software quality

Question	Yes	No
Has senior management made a commitment to develop quality software?		
Have you used CMMI to evaluate your organization's software development process?		
Has your company adopted a standard software development methodology?		
Does the methodology place a heavy emphasis on quality management and address how to define, measure, and refine the quality of the software development process and its products?		
Are software project managers and team members trained in the use of this methodology?		
Are software project managers and team members held accountable for following this methodology?		
Is a strong effort made to identify and remove errors as early as possible in the software development process?		
Are both static and dynamic software testing methods used?		
Are white-box testing and black-box testing methods used?		
Has an honest assessment been made to determine if the software being developed is safety critical?		
If the software is safety critical, are additional tools and methods employed, and do they include the following: a project safety engineer, hazard logs, safety reviews, formal configuration management systems, rigorous documentation, risk analysis processes, and the FMEA technique?		

Source Line: Course Technology/Cengage Learning.

Summary

- Demand for high-quality software is increasing
- Developers are under extreme pressure to reduce time to market of products
- Software product liability claims are frequently based on:
  - Strict liability
  - Negligence
  - Breach of warranty
  - Misrepresentation
- Software development methodology
  - Defines activities in the development process
  - Defines individual and group responsibilities
  - Recommends specific techniques
  - Offers guidelines for managing product quality

- CMMI
  - Defines five levels of software development maturity
- Safety-critical system
  - Failure may cause injury or death
- ISO 9001 standard is a guide to quality products, services, and management
- Failure mode and effects analysis (FMEA) is an important technique used to develop ISO 9001-compliant quality systems

Activity:

Directions: Fill in the blanks with the correct and most appropriate answer.

1. _____ are products such as statements of requirements, flowcharts and user documentation.

2. Negligence is failure to do what a reasonable _____ would do, or doing something that a reasonable _____ would not do.

3. Warranty assures buyers or lessees that a product meets certain _____ of quality.

4. Breach of warranty claim is when the product fails to meet the _____ of its warranty.

5. Black-box testing is used when the tester has no _____ of code.

6. White-box testing is testing all possible _____ paths in the software unit, with thorough knowledge of the _____.

7. Consequences of _____ _____ in certain systems can be deadly.

8. N-version programming involves the execution of a series of _____ instructions simultaneously by two different systems.

9. Reliability is the probability of a component or system performing without _____ over its product life.

10. Software development methodology defines _____ in the development process.

Chapter 8: The Impact of Information Technology on Productivity and Quality of Life

Objectives

As you read this chapter, consider the following questions:

- What impact has IT had on the standard of living and worker productivity?
- What is being done to reduce the negative influence of the digital divide?
- What impact can IT have on improving the quality of healthcare and reducing its costs?
- What ethical issues are raised because some entities can afford to make significant investments in IT while others cannot and thus are blocked in their efforts to raise productivity and quality?

The Impact of IT on the Standard of Living and Worker Productivity

- Gross domestic product (GDP)
  - Measurement of the material standard of living
  - Equals total annual output of a nation's economy
- Standard of living in U.S. and developed countries
  - Has improved for a long time
  - Rate of change varies as a result of business cycles
- Productivity
  - Amount of output produced per unit of input
  - Measured in many different ways
- United States
  - Labor productivity growth 2% annually
  - Living standards have doubled about every 36 years
  - Modern management techniques and automated technology increase productivity
- Innovation
  - Key factor in productivity improvement
  - IT has an important role

IT Investment and Productivity

- Relationship between IT investment and productivity growth is complex
  - Rate of productivity from 1995 to 2005 is only slightly higher than the long-term U.S. rate

  - Possible lag time between:
    - Application of innovative IT solutions
    - Capture of significant productivity gains
- Other factors besides IT influence worker productivity rates
- Difficult to quantify how much the use of IT has contributed to worker productivity
- Factors that affect national productivity rates
  - Business cycles of expansion and contraction
  - Outsourcing to contractors can skew productivity
  - Regulations make it easier to hire and fire workers
  - More competitive markets for goods and services
  - Difficult to measure output of some services
  - IT investments don't always yield tangible results

TABLE 8-1 Fundamental drivers for productivity performance

Reduce the amount of input required to produce a given output by:	Increase the value of the output produced by a given amount of input by:
Consolidating operations to better leverage economies of scale	Selling higher-value goods
Improving performance by becoming more efficient	Selling more goods to increase capacity and use of existing resources

Source Line: Course Technology/Cengage Learning.

- Telework/Telecommuting
  - Employee works away from the office
  - Advances in technology enable communications
  - Highly skilled workers demand more flexibility
  - Laws passed to encourage telework
  - Organizations must prepare guidelines and policies
  - Some positions are not suited to telework
  - Some individuals are not suited to be teleworkers

TABLE 8-2 Advantages/disadvantages of teleworking for employees

Advantages	Disadvantages
People with disabilities who otherwise find public transportation and office accommodations a barrier to work may now be able to join the workforce.	Some employees are unable to be productive workers away from the office.
Teleworkers avoid long, stressful commutes and gain time for additional work or personal activities.	Teleworkers may suffer from isolation and may not really feel "part of the team."
Telework minimizes the need for employees to take time off to stay home to care for a sick family member.	Workers who are out of sight also tend to be out of mind. The contributions of teleworkers may not be fully recognized and credited.
Teleworkers have an opportunity to experience an improved work/family balance.	Teleworkers must guard from working too many hours per day because work is always there.
Telework reduces ad hoc work requests and disruptions from fellow workers.	The cost of the necessary equipment and communication services can be considerable if the organization does not cover these.

Source Line: Course Technology/Cengage Learning.

TABLE 8-3 Advantages/disadvantages of teleworking for organizations

Advantages	Disadvantages
As more employees telework, there is less need for office and parking space; this can lead to lower costs.	Allowing teleworkers to access organizational data and systems from remote sites creates potential security issues.
Allowing employees to telework can improve morale and reduce turnover.	Informal, spontaneous meetings become more difficult if not impossible.
Telework allows for the continuity of business operations in the event of a local or national disaster and supports national pandemic-preparedness planning.	Managers may have a harder time monitoring the quality and quantity of the work performed by teleworkers, wondering, for instance, if they really "put in a full day."
The opportunity to telework can be seen as an additional perk that can help in recruiting.	Increased planning is required by managers to accommodate and include teleworkers.
There may be an actual gain in worker productivity.	There are additional costs associated with providing equipment, services, and support for people who work away from the office.
Telework can decrease an organization's carbon footprint by reducing daily commuting.	Telework increases the potential for lost or stolen equipment.

Source Line: Course Technology/Cengage Learning.

The Digital Divide

- Standard of living
  - Level of material comfort measured by the goods, services, and luxuries available

- Digital divide
  - Gulf between those who do/don't have access to:
    - Cell phones
    - Personal computers
    - The Internet
  - Gulf among age groups, economic classes, and cities/rural areas
- Digital divide must be bridged to improve resolution of:
  - Health emergencies
  - Crime emergencies
  - Other emergencies
- Access to IT and communications technology:
  - Enhances learning
  - Provides educational and economic opportunities
  - Influences cultural, social, and political conditions
- Education Rate (E-Rate) program
  - Created by the Telecommunications Act of 1996
  - Goal to help schools and libraries obtain:
    - Access to state-of-the-art services and technologies
    - Discounted rates
  - Supported with up to $2.25 billion per year from fees charged to telephone customers
  - Administered by the Universal Service Administrative Company (USAC)
  - Has not gone well but continues today
- Low-cost computers for developing countries
  - One Laptop per Child (OLPC)
    - Provides low-cost laptop computers for education
  - Classmate PC from Intel
  - Eee notebook from Asus
- Mobile phone
  - Tool to bridge the digital divide
  - Costs less than PC and more broadly available

The Impact of IT on Healthcare Costs

- Rapidly rising cost of healthcare is major challenge
  - Spending increasing at 6.3% per year
  - Grow from $2.6 trillion to $4.6 trillion by 2019
- Increase (above inflation) due to new medical technology
  - Diagnostic procedures and treatments
  - Patients sometimes overuse medical resources

- Patient awareness must be raised
- Technology costs must be managed
- Improved use of IT can lead to cost reductions

Electronic Health Records

- Electronic health record (EHR)
  - Computer readable record of health-related information on an individual: patient demographics, medical history, family history, immunization records, lab data, health problems, progress notes, medications, vital signs, and radiology reports
  - Summary of health information generated by each patient encounter in any healthcare delivery setting
  - Effective use of EHR improves patient care and reduces costs
- Lack of patient data transparency results in:
  - Diagnostic and medication errors
  - Ordering of duplicate tests
  - Compromise of patient safety
  - At least 98,000 people die in hospitals each year due to preventable medical mistakes
- Health Information Technology for Economic and Clinical Health Act (HITECH)
  - Requires government to develop standards for nationwide exchange and use of health information
  - Provides $20 billion in incentives
  - Saves $10 billion through improvements in quality of care
  - Strengthens protection of identifiable health information

Use of Mobile and Wireless Technology in the Healthcare Industry

Healthcare industry is a leader in adopting mobile and wireless technology

- Means to access/update EHR at bedsides
- Scan barcodes to match patient with medications
- Communicate with healthcare employees

Telemedicine

- Employs modern telecommunications and information technologies
- Provides medical care to people who live far away from healthcare providers

- Store-and-forward telemedicine
  - Acquires data, sound, images, and video from patient and transmits to medical specialist for evaluation at a later time
  - Does not require presence of patient
- Live telemedicine
  - Requires the presence of patient and healthcare provider at the same time
  - Involves a video conference link between the two sites
- Use of telemedicine raises new ethical issues:
  - Must physicians providing advice to patients at remote location be licensed at that location?
  - Must healthcare system be required to possess a license from a state in which it has a virtual facility?
  - Must minimum set of technology standards be met?
  - What sort of system certification and verification is necessary?
  - Does patient involvement with remote doctors have negative impact on the local doctor's relationship?

Medical Information Web Sites for Laypeople

- People need reliable information on a wide range of medical topics to:
  - Learn more about healthcare services
  - Take more responsibility for their health
- Web sites are not substitutes for professional medical advice, diagnosis, or treatment
- Some healthcare providers and employers offer online tools that go beyond basic health information

TABLE 8-5 Health information Web sites

URL	Site
www.americanheart.org	American Heart Association
www.cancer.org	American Cancer Society
www.cdc.gov	Centers for Disease Control and Prevention
www.diabetes.org	American Diabetes Association
www.heartburn.about.com	Information on the causes of heartburn and how to prevent it
www.heartdisease.about.com	Basic information about heart disease and cardiology
www.medicinenet.com	Source for medical information on a variety of topics, including symptoms, procedures, tests, and medications, as well as a medical dictionary
www.nia.nih.gov/Alzheimers	National Institute on Aging—Alzheimer's Disease Education and Referral Center
www.niddk.nih.gov	National Institute of Diabetes and Digestive and Kidney Diseases
www.oncolink.upenn.edu	Abramson Cancer Center of the University of Pennsylvania
www.osteo.org	National Institutes of Health—Osteoporosis and Related Bone Diseases National Resource Center
www.urologychannel.com	Information about urologic conditions, including erectile dysfunction, HIV, AIDS, kidney stones, and STDs; site contains overviews, symptoms, causes, diagnostic procedures, and treatment options
www.webmd.com	Access to medical reference material and online professional publications

Source Line: Course Technology/Cengage Learning.

Summary

- Gross national product (GNP) measures material standard of living
- Progressive management uses IT to innovate products, processes, and services
- Telework opportunities can be used to:
  - Reduce costs
  - Increase productivity
  - Reduce organization's carbon footprint
  - Prepare for potential local or widespread disasters
- The digital divide exists:
  - Between more and less developed countries

- Within countries, among:
  - Age groups
  - Economic classes
  - People who live in cities versus those in rural areas
- New information technologies can be used with little capital cost to reduce the digital divide
- Healthcare costs are soaring out of control
  - 6.3% annual growth rate
  - Will reach $4.6 trillion by 2019
- Improved use of IT in the healthcare industry can lead to significantly reduced costs
  - Electronic health records (EHRs)
  - Telemedicine
  - Web-based health information

Activity

Directions: Identify the following. Write your answer on the space provided.

_____1. Measurement of the material standard of living and is equal to the total annual output of a nation's economy.

_____2. Amount of output produced per unit of input.

_____3. Key factor in productivity improvement.

_____4. Level of material comfort measured by the goods, services, and luxuries available.

_____5. Gulf between those who do/don't have access to: cell phones, personal computers, and the Internet.

_____6. Computer readable record of health-related information on an individual: patient demographics, medical history, family history, immunization records, lab data, health problems, progress notes, medications, vital signs, and radiology reports.

_____7. Measures the material standard of living.

_____8. Created by the Telecommunications Act of 1996 whose goal is to help schools and libraries obtain access to state-of-the-art services and technologies and discounted rates.

_____9. Tool to bridge the digital divide and costs less than PC and more broadly available.

_____10. Employs modern telecommunications and information technologies and provides medical care to people who live far away from healthcare providers.

Chapter 9: Social Networking

Objectives
As you read this chapter, consider the following questions:

- What are social networks, how do people use them, and what are some of their practical business uses?
- What are some of the key ethical issues associated with the use of social networking Web sites?
- What is a virtual life community, and what are some of the ethical issues associated with such a community?

What Is a Social Networking Web Site?

- Creates an online community of Internet users that eliminates barriers created by time, distance, and cultural differences
- Allows people to interact with others online by sharing opinions, insights, information, interests, and experiences
- Members may use the site to interact with friends, family members, and colleagues they already know
- Members may also wish to develop new personal and professional relationships

TABLE 9-1 Popular social networking Web sites

Social networking Web site	Description	Estimated unique monthly visitors
Facebook	Social networking site for keeping up with friends, uploading photos, sharing links and videos, and meeting new people online	700 million
Twitter	A real-time information service for friends, family members, and coworkers looking to stay connected through the exchange of messages that are a maximum of 140 characters	200 million
LinkedIn	Business-oriented social networking site used for professional networking; users create a network made up of people they know and trust in business.	100 million
MySpace	General social networking Web site used by teenagers and adults worldwide; allows members to communicate with friends via personal profiles, blogs, and groups, as well as to post photos, music, and videos to their personal pages	80.5 million
Ning	Platform that enables users to create their own social network following a simple process to name the network, choose a color scheme, and allow for unique profile questions; serves as a portal to access tens of thousands of user-created social networks	60 million
Tagged	Social network with a focus on helping members meet new people; suggests new friends based on shared interests; allows members to browse people, share tags and virtual gifts, and play games	25 million
Google Plus[13]	Social network operated by Google that integrates social services such as Google Profiles and Google Buzz, and introduces new services such as Circles (enables users to organize contacts into groups for sharing), Hangouts (URLs used to facilitate group video chat), Sparks (enables users to identify topics in which they are interested), and Huddles (allows instant messaging within Circles)	25 million

(*Continued*)

Source Line: "Top 15 Most Popular Social Networking Websites/July 2011," eBiz/MBA, www.ebizmba.com/articles/social-networking-websites. "Google Plus Reaches 25 Million Users, Activity Declines," Search Engine Journal, © August 3, 2011, www.searchenginejournal.com/google-plus-reaches-25-million-users-activity-declines/31500.

- Endless range of interests and a wide range of social networking Web sites catering to those interests
- Over 314.5 million social network users worldwide
- Average visitor spends almost six hours per month
- Popularity increasing mostly rapidly among those aged 50 and older

Business Applications of Online Social Networking

- Social network advertising
  - Uses social networks to communicate and promote the benefits of products and services
- Social network advertising strategies
  - Direct advertising
    - Banner ads on social networking Web site
  - Advertising using an individual's network of friends
    - People frequently make decisions based on input from their close group of friends
    - Ethical issues with exploiting an individual's personal relationships for the financial benefit of a company
  - Indirect advertising through groups
    - Interested users can join by becoming "fans"
    - Fans gained in this manner may not remain loyal
  - Company-owned social networking Web site
    - Users can talk about what new products, services, or improvements they would like to see
  - Viral marketing
    - Users pass along marketing message to others, creating the potential for exponential growth

The Use of Social Networks in the Hiring Process

- 89% of recruiters use some form of social media in the recruiting process
- Employers can and do look at the social networking profiles of job candidates when hiring

- Companies may reject candidates who post:
  - Information about their drinking or drug use
  - Provocative or inappropriate photos
  - Discriminatory remarks relating to race, gender, or religion
  - Confidential information
- Employer cannot legally screen applicants based on race or ethnicity, but:
  - Members of social networking Web sites frequently provide sex, age, marital status, sexual orientation, religion, and political affiliation data
  - Personal photos may reveal a disability or user's race or ethnicity
  - Individuals may reveal data that are protected by civil rights legislation

Use of Social Media to Improve Customer Service

- Consumers use social networks to share their experiences, both good and bad, with others
- Also seek help and advice on how to use products more effectively and how to deal with special situations
- Unless organizations monitor social networks, customers are left to resolve questions and issues on their own, risking loss of customers and future sales

Social Shopping Web Sites

- Combine two highly popular online activities: shopping and social networking
- Shoppers and sellers can share information and make recommendations while shopping online
- Revenue is generated through retailer advertising or by sharing with retailers data about their members' likes and dislikes
- Retailers can design product improvements based on input and get ideas for new product lines
- Great way for small businesses to boost sales

TABLE 9-3 Sample of social shopping Web sites

Social shopping site	Description
Buzzillions	Product review Web site with over 15 million reviews across a wide range of products, with product rankings based on feedback from customers
Crowdstorm	Price comparison shopping resource that aggregates product information from various online buyers guides, reviews, and blog postings
JustBoughtIT!	Facebook and Twitter app for capturing product recommendations from the online community; users can post a photo or screenshot online, share their purchases, and comment on what others are buying.
Kaboodle	Social shopping site where members can discover, recommend and share new products, provide advice, share feedback, get discounts, and locate bargains
MyDeco	Site with a focus on interior design and home décor; users can mock up virtual rooms using their favorite products
OSOYOU	UK-based social shopping site for women with an interest in fashion and beauty products

Source Line: Course Technology/Cengage Learning.

Social Networking Ethical Issues

- Ethical issues for social networking Web sites are:
  - Cyberbullying
  - Cyberstalking
  - Sexual predators
  - Uploading inappropriate material
- Cyberbullying
  - Harassment, torment, humiliation, or threatening of one minor by another minor or group of minors via the Internet or cell phone
  - Cyberbullying can become so intense, child commits suicide

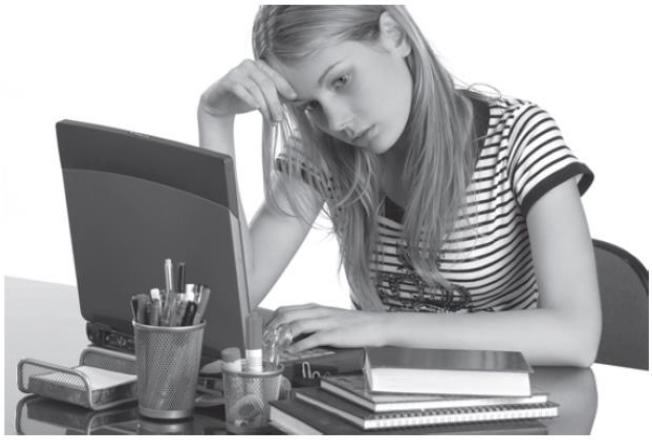

FIGURE 9-2 Cyberbullying is more common among teenage females
Credit: Image copyright Ana Blazic, 2009. Used under license from Shutterstock.com.

- Numerous forms of cyberbullying
  - Sending mean-spirited or threatening messages
  - Sending thousands of text messages to victim's cell phone and running up a huge cell phone bill
  - Impersonating victim and sending inappropriate messages to others
  - Stealing victim's password and modifying his or her profile to include racist, homophobic, sexual, or other inappropriate data that offends others or attracts the attention of undesirable people
  - Posting mean, personal, or false information about the victim in the cyberbully's blog
  - Creating a Web site whose purpose is to humiliate or threaten the victim
  - Taking inappropriate photos of the victim and either posting online or sending to others via cell phone
  - Setting up an Internet poll to elicit responses to embarrassing questions regarding victim
  - Sending inappropriate messages while playing interactive games
- Cyberstalking
  - Threatening behavior or unwanted advances using the Internet or online and electronic communications
  - Adult version of cyberbullying
  - Can escalate into:
    - Abusive or excessive phone calls
    - Threatening or obscene mail
    - Trespassing
    - Vandalism
    - Physical stalking
    - Physical assault

    - Over three dozen states have laws prohibiting cyberstalking
    - Current federal statues address some forms of cyberstalking, but there are large gaps in federal and state law
- Encounters with sexual predators
    - Some social networking Web sites are criticized for not protecting minors from sexual predators
        - MySpace banned 90,000 registered sex offenders from its site
    - Legislators are pushing social networking Web sites to adopt stronger safety measures
- Uploading of inappropriate material
    - Social networking Web sites have policies against uploading videos depicting violence or obscenity
    - Most social networking Web sites have terms of use agreements that give the sites the right to delete material and terminate users accounts that violate their policy
    - Most Web sites do not have sufficient resources to review all material posted

Online Virtual Worlds

- Virtual world is a shared multimedia, computer-generated environment in which users represented by avatars can act, communicate, create, retain ownership of what they create, and exchange assets with each other
    - Massively multiplayer online game (MMOG) is multiplayer video game capable of supporting hundreds or even thousands of concurrent players
        - Massively multiplayer online role playing game (MMORPG) provides huge online world in which players take on the role of a character and control that character's action
- Avatars can do everything one can do in real life
    - Shop, hold jobs, run for political office
    - Develop relationships with other avatars
    - Start up new businesses
    - Engage in criminal activities

Crime in Virtual Worlds

- Should law enforcement—real or virtual—get involved in acts that occur in virtual worlds?
- Criminal acts in a virtual world:
    - Can be clearly illegal, such as trafficking in actual drugs or stolen credit cards

  - May not be real-life crime, such as virtual muggings and sex crimes that can cause real life anguish
  - May be in the gray area, for example, unfair operation of virtual casinos
- Virtual worlds have rules against offensive behavior in public, such as using racial slurs or performing overtly sexual actions, but:
  - Consenting adults can travel to private areas and engage in socially unacceptable behavior
  - Bad deeds done online can often be mediated by game administrators based on rules of the game

Educational and Business Uses of Virtual Worlds

- New Media Consortium (NMC)
  - International consortium of hundreds of organizations
  - Explores new media and technologies to improve teaching, learning, and creative expression
  - Also builds custom virtual learning worlds, simulations, and learning games
- Second Life Work Microsites
  - Enable businesses and government agencies to use Second Life for virtual meetings, events, training, and simulations
  - Stimulates engaged, collaborative learning to augment their traditional curriculum

Summary

- Social networking Web sites
  - Create an online community of Internet users
  - Break down barriers created by time, distance, and cultural differences
  - Allow people to interact with others online by sharing opinions, insights, information, interests, and experiences
- Social network advertising uses social networks to inform, promote, and communicate the benefits of products and services
  - Social network advertising strategies
  - Direct advertising
  - Advertising using network of friends
  - Indirect advertising through groups
  - Advertising via company-owned Web sites
  - Viral marketing

- Employers look at the social network profiles of job candidates when hiring
- Consumers use social networks to share their experiences and seek help and advice
- Unless organizations monitor social networks, customers are left to resolve questions and issues on their own, risking loss of customers and future sales
- Ethical issues for social networking Web sites are:
  - Cyberbullying
  - Cyberstalking
  - Sexual predators
  - Uploading inappropriate material
- Online virtual world is a computer-simulated world
  - Visitor can move in three-dimensional space
  - Visitor can communicate and interact with other visitors
  - Visitor can manipulate elements of the simulated world

Activity

Directions: Choose the most correct answer from the given set.

New Media Consortium (NMC)	Social Shopping Web Sites	Online Virtual Worlds	Cyberbullying	Revenue
Social network advertising	Social Networking Web Site	Massively Multiplayer Online Role Playing Game (MMORPG)	Cyberstalking	Avatars

_____1. Creates an online community of Internet users that eliminates barriers created by time, distance, and cultural differences.

_____2. A shared multimedia, computer-generated environment in which users represented by avatars can act, communicate, create, retain ownership of what they create, and exchange assets with each other.

_____3. International consortium of hundreds of organizations that explores new media and technologies to improve teaching, learning, and creative expression.

_____4. Combine two highly popular online activities: shopping and social networking.

_____5. Generated through retailer advertising or by sharing with retailers data about their members' likes and dislikes.

_____6. Harassment, torment, humiliation, or threatening of one minor by another minor or group of minors via the Internet or cell phone.

_____7. Provides huge online world in which players take on the role of a character and control that character's action.

_____8. Uses social networks to communicate and promote the benefits of products and services.

_____9. Can do everything one can do in real life.

_____10. Threatening behavior or unwanted advances using the Internet or online and electronic communications.

Chapter10: Ethics of IT Organizations

Objectives

As you read this chapter, consider the following questions:

- What are contingent workers, and how are they employed in the information technology industry?
- What key ethical issues are associated with the use of contingent workers, including H-1B visa holders and offshore outsourcing companies?
- What is whistle-blowing, and what ethical issues are associated with it?
- What is an effective whistle-blowing process?
- What measures are members of the electronics manufacturing industry taking to ensure the ethical behavior of the many participants in their long and complex supply chains?
- What is green computing, and what are organizations doing to support this initiative?

Key Ethical Issues for Organizations

Ethical topics are pertinent to organizations in the IT industry and organizations that make use of IT

- Use of nontraditional workers
- Whistle-blowing
- Green computing
- ICT code of ethics

The Need for Nontraditional Workers

- Bureau of Labor Statistics (BLS) forecast
  - Network systems and data communications analysts will be 2nd fastest growing occupation from 2008-2018
  - Employment of computer software engineers will grow 34%
- Concern about a shortfall in the number of U.S. workers to fill these positions

- Several IT positions in the top-ten paid majors for 2010-2011 bachelor's degree graduates
- Long-term shortage of IT workers
  - Employers turning to nontraditional sources

- Sources include:
  - Contingent workers
  - H-1B workers
  - Outsourced offshore workers
- Ethical decisions about whether to:
  - Recruit new/more workers from these sources
  - Develop their own staff to meet their needs

Contingent Workers

- Contingent work is a job situation in which an individual does not have an explicit or implicit contract for long-term employment
- Contingent workers include:
  - Independent contractors
  - Temporary workers through employment agencies
  - On-call or day laborers
  - On-site workers provided by contract firms
- Needed for pronounced IT staffing fluctuations
- Workers hired for the life of the project only
- Sources
  - Temporary agencies
  - Employee leasing
  - Consulting organizations
- Firms that provide temporary help:
  - Recruit, train, and test their employees in a wide range of job categories and skill levels
  - Assign them to clients

TABLE 10-2 Large IT consulting firms

Firm	Headquarters
Accenture	Dublin, Ireland
Deloitte Touche Tohmatsu	New York, New York
Electronic Data Systems	Plano, Texas
Ernst & Young	New York, New York
HP Enterprise Business	Palo Alto, CA
IBM Global Business Services	Armonk, New York
Infosys	Bangalore, India
KPMG	Amstelveen, Netherlands
Tata Consultancy Services	Mumbai, India
Wipro Technologies	Bangalore, India

Source Line: Course Technology/Cengage Learning.

- Employee leasing
  - Business outsources all or part of its workforce to a professional employer organization
  - Subject to special regulations regarding workers' compensation and unemployment insurance
- Co-employment relationship
  - Two employers have actual or potential legal rights and duties with respect to the same employee or group of employees
- Advantages of using contingent workers
  - Business does not pay for benefits
  - Can continually adjust the number of contingent workers to stay consistent with its business needs
  - Does not customarily incur training costs
- Disadvantages of using contingent workers
  - Workers may lack a strong relationship with the firm
    - Low commitment to the company and its projects
    - High turnover rate
  - Workers gain valuable practical experience working within a company's structure and culture
    - Lost when workers depart at the project's completion
- When deciding to use contingent workers:
  - Recognize the trade-off between:
    - Completing a single project quickly and cheaply
    - Developing people in the organization

- When staffing is truly temporary:
  - Use of contingent workers is a good approach
- Think twice about using contingent workers:
  - When they are likely to learn corporate processes and strategies that are key to the company's success
    - Worker's next assignment may be with major competitor

- Deciding when to use contingent workers
- Can raise ethical and legal issues
- Potential liability for:
  - Withholding payroll taxes
  - Payment of employee retirement benefits
  - Payment of health insurance premiums
  - Administration of workers' compensation
- Deciding when to use contingent workers (cont'd.)
  - Can be viewed as permanent employees by:
    - Internal Revenue Service
    - Labor Department
    - State workers' compensation agency
    - State unemployment agencies
  - *Vizcaino v. Microsoft* lawsuit
    - Deciding factor is degree of control company exercises over employees
    - Employers must exercise care in the treatment of contingent worker

TABLE 10-3 Manager's checklist for the use of contingent employees

Question	Yes	No
Have you reviewed the definition of an employee in your company's policies and pension plan documents to ensure it is not so broad that it encompasses contingent workers, thus entitling them to benefits?		
Are you careful not to use contingent workers on an extended basis? Do you make sure the assignments are finite, with break periods in between?		
Do you use contracts that specifically designate workers as contingent workers?		
Are you aware that the actual circumstances of the working relationship determine whether a worker is considered an employee in various contexts, and that a company's definition of a contingent worker may not be accepted as accurate by a government agency or court?		
Do you avoid telling contingent workers where, when, and how to do their jobs and instead work through the contingent worker's manager to communicate job requirements?		
Do you request that contingent workers use their own equipment and resources, such as computers and email accounts?		
Do you avoid training your contingent workers?		
When leasing employees from an agency, do you let the agency do its job? Do you avoid asking to see résumés and getting involved with compensation, performance feedback, counseling, or day-to-day supervision?		
If you lease employees, do you use a leasing firm that offers its own benefits plan, deducts payroll taxes, and provides required insurance?		

Source Line: Course Technology/Cengage Learning.

H-1B Workers

- Temporary work visa
  - U.S. Citizenship and Immigration Services (USCIS)
  - For people who work in specialty occupations
- H-1B workers
  - Meet critical business needs
  - Have essential technical skills and knowledge not readily found in the U.S.
  - Employers must pay H-1B workers the prevailing wage for the work being performed
- Maximum continuous period of six years
  - After six years, the foreign worker must remain outside the United States for one year before another H-1B petition can be approved

- Continued use of H-1B workers
  - Symptom of a larger, more fundamental problem
  - U.S. not developing sufficient IT employees
- Top five outsourcing countries
  - India
  - China
  - Canada
  - Philippines
  - Korea
- Federal cap of 65,000 for number of H-1B visas
  - Applies only to certain IT professionals
  - Large number of workers are exempt from cap
- English as a second language
  - Workers who are not fluent in English:
    - May find it difficult and uncomfortable to participate
    - May create their own cliques
    - May stop trying to acclimate
    - Can hurt a project team's morale and lead to division
- Managers and coworkers should:
  - Strive to help improve H-1B workers' English skills and cultural understanding
  - Be sensitive to workers' heritage and needs
- H-1B application process
  - Employer making job offer must also offer sponsorship
  - Application has two stages
    - Labor Condition Attestation (LCA)
    - H-1B visa application
  - If H-1B are more than 15% percent of company's workforce:
    - Must prove that it first tried to find U.S. workers
    - Must prove not hiring H-1B after laying off similar U.S. worker
- American Competitiveness in the Twenty-First Century Act (2000)
  - Allows current H-1B holders to start working for employers as soon as their petitions are filed
- Using H-1B workers instead of U.S. workers
  - Good for short-term hiring
  - Long-term hiring
    - Lessens incentive to educate and develop U.S. workforces
    - Does nothing to develop strong core of permanent U.S. IT workers needed in future

- Potential exploitation of H-1B workers

- Salary abuse by unethical companies
- Some H1-B workers are paid $10,000 to $30,000 less than U.S. workers in the same job
- Visa Reform Act (2004)
  - Defined a modified wage-rate system
- At end of the six-year visa term:
  - If no green card, firm loses worker
  - Suddenly unemployed worker must return home

B - 1 Visa Controversy

- B-1 visitor visa for people who wish to enter U.S. temporarily:
  - For pleasure or medical treatment
  - To travel for short periods of time to consult with business associates; attend convention or conference; negotiate a contract; or install or maintain machinery
- B-1 visa faster, easier, and cheaper to obtain
  - Lot of gray area in the use of B-1 visas

Outsourcing

- Outsourcing
  - Approach to meeting staffing needs
  - Long-term business arrangement
    - Company contracts with an outside organization that has expertise in providing a specific function
- Rationale
  - Co-employment legal problems are minimal
  - Lower costs
  - Obtain strategic flexibility
  - Keep staff focused on core competencies

Offshore Outsourcing

- Variation of outsourcing
  - Services provided by an organization whose employees are in a foreign country
- Companies reduce labor costs
- Increasing in IT industry

- As key processes move offshore, U.S. IT providers are forced to lower prices
- Common to use offshore outsourcing for major programming projects

TABLE 10-5 Most attractive offshoring destinations (Based on A.T. Kearney rating methodology)

Country
1. India
2. China
3. Malaysia
4. Egypt
5. Indonesia
6. Mexico
7. Thailand
8. Vietnam
9. Philippines
10. Chile

Source Line: A.T. Kearney, Inc., "A.T. Kearney's Global Services Location Index™," © 2011, www.atkearney.com/index.php/Publications/at-kearneys-global-services-location-index-volume-xiii-number-2-2010.html.

TABLE 10-6 Top-rated IT outsourcing firms according to the International Association of Outsourcing Professionals

Firm	Headquarters location
Accenture	Dublin, Ireland
Infosys Technologies	Bangalore, India
CSC	Falls Church, Virginia
Wipro Technologies	Bangalore, India
Capgemini S.A.	Paris, France
PCCW Solutions	Hong Kong

(*Continued*)

Firm	Headquarters location
CGI Group	Montreal, Quebec, Canada
HCL Technologies	New Delhi, India
ITC Infotech	Bangalore, India

Source Line: International Association of Outsourcing Professionals, "The 2011 Global Outsourcing 100," © 2011, www.iaop.org/Content/19/165/1793/Default.aspx.

- Pros and cons of offshore outsourcing
  - Low wages
    - Demand for offshoring driving up salaries
  - Dramatically speeds up development efforts
    - Make progress on a project around the clock
  - Can also result in new expenses
    - Additional time to select an offshore vendor
    - Additional costs for travel and communications
  - Same ethical issues as H1-B and contingent workers
  - Difficulty of communications over long distances and differences in culture and language
- Strategies for successful offshore outsourcing
  - Expertise in technologies involved in the project
  - Project manager speaks native language of employer
  - Large staff available
  - State-of-the-art telecommunications setup
  - High-quality on-site managers and supervisors

Whistle-Blowing

- Effort to attract public attention to a negligent, illegal, unethical, abusive, or dangerous act by a company
- Whistle-blower
  - Usually has personal or special knowledge
  - Risks own career
  - Might even affect lives of friends and family
  - Must choose between protecting society and remaining silent
- Protection laws allow employees to alert authorities to employer actions that are unethical, illegal, or unsafe or that violate specific public policies
  - No comprehensive federal law
  - Each law has different:
    - Filing provisions
    - Administrative and judicial remedies
    - Statutes of limitations
- False Claims Act (“Lincoln Law”)
  - Enacted during the Civil War
  - Enticed whistle-blowers to come forward
  - Offered a share of the money recovered
- Qui tam provision allows private citizen to file in name of government
- Violators are liable for three times the dollar amount the government is defrauded

- Provides strong whistle-blower protection
- Complexity requires advice of an attorney
- Whistle-blower protection for private-sector workers
  - Many states, not all, have laws that prevent workers from being fired because of an employee's participation in "protected" activities
- Whistle-blowers can file claims against their employers for retaliatory termination
- Whistle-blowers are entitled to jury trials
- If successful at trial, can receive punitive damage awards
- Dealing with a whistle-blowing situation
  - Assess the seriousness of the situation
  - Begin documentation
  - Attempt to address the situation internally
  - Consider escalating the situation within the company
  - Assess implications of becoming a whistle-blower
  - Use experienced resources to develop action plan
  - Execute the action plan
  - Live with the consequences

Green Computing

- To manufacture truly "green" products, companies must:
  - Produce product that requires less electricity
  - Reduce the amount of hazardous materials used
  - Increase amount of reusable or recyclable materials
  - Help consumers dispose of their products in an environmentally safe manner at the end of the product's useful life
- Personal computers and cell phones contain thousands of components composed of many different materials
  - Some harmful to humans and environment
  - Workers along the entire supply chain at risk
  - Users can also be exposed to these materials
- EPEAT (Electronic Product Environmental Assessment Tool)
  - Enables purchasers to evaluate, compare, and select electronic products
    - Based on a total of 51 environmental criteria
    - Products are ranked in three tiers of environmental performance
- European Restriction of Hazardous Substances Directive
  - Restricts use of many hazardous materials in computer manufacturing
- How to safely dispose of obsolete computers
  - Many states have recycling programs
  - Some manufacturers have developed programs

- Greenpeace environmental activist organization
  - Issues quarterly ratings of manufacturers according to the manufacturers' policies on toxic chemicals, recycling, and climate change
    - Manufacturers have long way to go to meet the high standards

ICT Industry Code of Conduct

- Electronic Industry Citizenship Coalition (EICC)
  - Promotes common code of conduct for ICT industry
  - Focuses on the areas of:
    - Worker safety and fairness
    - Environmental responsibility
    - Business efficiency
  - Coalition membership is voluntary
- Code of conduct defines performance, compliance, auditing, and reporting guidelines across five areas of social responsibility
- Guiding principles of social responsibility
  - Labor
    - Must uphold the human rights of workers
  - Health and safety
    - Must provide safe and healthy work environment
  - Environment
    - Adverse effects minimized
  - Management system
    - Ensures compliance with code
  - Ethics
    - Must uphold the highest standards of ethics

Summary

- Contingent workforce includes:
  - Independent contractors
  - Temporary workers through employment agencies
  - On-call or day laborers
  - On-site workers provided by contract firms

- Outsourcing
  - Long-term business arrangement
  - Contract for services with outside organization
  - Expertise in providing a specific function
- Whistle-blowing
  - Effort to attract public attention to negligent, illegal, unethical, abusive, or dangerous acts by company
  - Whistle-blowing process
    - Assess the seriousness of the situation
    - Begin documentation
    - Attempt to address the situation internally
    - Consider escalating the situation within the company
    - Assess the implications of becoming a whistle-blower
    - Use experienced resources to develop an action plan
    - Execute the action plan
    - Live with the consequences
- Green computers
  - Use less electricity
  - Include fewer hazardous materials
  - Contain reusable or recyclable material
- Manufacturers must help consumers:
  - Dispose of products in an environmentally safe manner at the end of the product's useful life
- EPEAT (Electronic Product Assessment Tool)
  - Purchasers can evaluate, compare, and select
  - Based on 51 environmental criteria

Activity

Enumeration

1. Key Ethical Issues for Organizations

_____

_____

_____

_____

2. Top five outsourcing countries

_____

_____

_____

_____

_____

3. Pros and cons of offshore outsourcing

_____

_____

_____

_____

_____

_____

4. Characteristics of a Whistle-blower

_____

_____

_____

_____