Professional Practices

“The Computing Profession”

Contents

- Profession
- Fundamental characteristics of a profession
- Structure of computing profession
- Ethics
- Professional Ethics
- Professional codes of conduct
- Ten Commandments of computer ethics
- Applying codes of conduct (Case Studies)

Profession

"A paid occupation, especially one that involves prolonged training and a formal qualification"

Profession

- A formal education is one where you would go to a college or university for an actual degree.
- An informal education is simply learning a trade from someone else. It's possible to have a formal education and an informal education.
- The formal education is what most employers would prefer to see because it is easier to prove. Having a degree in a specific field will mean that you have certain knowledge that will translate into a better paying job and the company that's employing you getting a qualified person for the job.

Profession

- An informal education is what many people end up having. You work under someone who has a degree or has been doing it for enough years to be knowledgeable about the subject.
- Many car mechanics and other "trade" skills usually have an informal education as to what they're doing.
- Informal education can also be referred to as life experience. After going through life for so many years, you'll naturally acquire some knowledge about different things that you may not even learn after going through a formal education.

Fundamental characteristics of a profession

- **Great responsibility**
  - Professionals deal in matters of vital importance to their clients and are therefore entrusted with grave responsibilities and obligations.
  - Given these essential obligations, professional work typically involves circumstances where carelessness, inadequate skill, or breach of ethics would be significantly damaging to the client and/or his fortunes.

Fundamental characteristics of a profession

- **Accountability**
  - Professionals hold themselves ultimately accountable for the quality of their work with the client.
  - The profession may or may not have mechanisms in place to reinforce and ensure adherence to this principle among its members.

Fundamental characteristics of a profession

- **Based on specialized, theoretical knowledge**
  - Professionals render specialized services based on theory, knowledge, and skills that are characteristic to their profession and generally beyond the understanding or capability of those outside of the profession.
  - Sometimes, this specialization will extend to access to the tools and technologies used in the profession (e.g. medical equipment).

Fundamental characteristics of a profession

- **Institutional preparation**
  - Professions typically require a significant period of hands-on, practical experience in the protected company of senior members before candidates are recognized as professionals.
  - After this provisional period, ongoing education toward professional development is compulsory.

Fundamental characteristics of a profession

- **Ethical constraints**
  - Due to the other characteristics on this list, there is a clear requirement for ethical constraints in the professions.
  - Professionals are bound to a code of conduct or ethics specific to the distinct profession.
  - Professionals also aim toward a general body of core values, which are centered upon the client's benefit and best interests.

Fundamental characteristics of a profession

- **Merit-based**
  - In a profession, members achieve employment and success based on merit rather than on corrupted ideas such as social principle, mandated support, or extortion.
  - Therefore, a professional is one who must attract clients and profits due to the merits of his work.
  - In the absence of this characteristic, issues of responsibility, accountability, and ethical constraints become irrelevant, negating any otherwise-professional characteristics.

10 things that define a true professional

- Put customer satisfaction first
- Make expertise your specialty
- Do more than expected
- Do what you say and say what you can do
- Communicate effectively
- Follow exceptional guiding principles
- Praise your peers not yourself
- Share your knowledge
- Say thank you
- Keep a smile on your face and the right attitude in your heart

Structure of computing profession

- The computing profession has a two tier structure.
- At the first level, there are the institutions, that is, the chartered professional bodies, each of which covers a single or several closely related computing disciplines. Examples are PIEAS, NUST etc.

Structure of computing profession

- The second level body in computing is the computing council, a chartered body which recognizes certain computing institutions as its nominated bodies.
- By recognizing a computing institution means that Computing council is satisfied with its standard of education.

Structure of computing profession

- Computing council acts as an umbrella body and represents the interests of the computing profession as a whole.
- National Computing Education Accreditation Council (NCEAC) is a professional body and constitutional federal institution for accreditation of computing education and regulation of computing profession in Pakistan.

Structure of computing profession

- NCEAC is recognized accreditator of computing programs in Pakistan.
- It ensures the quality of education students received in universities and institutions.
- It stimulates innovation in applied sciences, computing, Engineering and technology education.

Ethics

- Ethics is the study of right and wrong in relation to human actions. It includes
  - ***Meta-ethics:*** study of general principles from which ethical systems can be built.
  - ***Moral theory:*** ethical systems, consisting of the **criteria** to decide whether individual actions are right and wrong.
  - ***Practical ethics:*** application of ethical systems to the analysis of particular situations.

What is Professional Ethics

- One's conduct of behavior and practice when carrying out professional work, e.g., consulting, researching, teaching.
- The principles and standards that guide members of a particular profession in their interactions with internal & external stakeholders.

Professional Ethics

- Professional Ethics must take into accounts:
  - Relations between professionals and clients
  - Relation between profession and society
  - Relations among professionals
  - Relations between employee and employer

Why professional ethics?

- Awareness of professional ethics is gaining importance with time.
- **Decision making** process in the work place is a complex phenomena.
- The professional ethics provide a way of **simplifying** that decision making process.

Professional code of conduct

- One of main characteristic of profession is that the professional body establishes and enforces a code of conduct on its members.
- As far as computing is concerned, most code of conducts established by ACM and IEEE undergo major revisions with the passage of time.
- All previous code of conducts are recently replaced by “Software Engineering Code of Ethics and Professional Practice” developed jointly by the ACM and IEEE Computer society.

Professional code of conduct

- It outlines 8 principles of computing ethics: The obligation of the computing professional to the
  - general public
  - the client and employer
  - the product
  - the profession
  - Colleagues
  - the engineer himself or herself
  - the ethical management of software engineering projects.

Ten Commandments of Computer ethics

- The Ten Commandments of Computer Ethics were created in 1992 by the Computer Ethics Institute.
  - Not use a computer to harm other people. This is the foundation for computer ethics.
  - Not interfere with other people's computer work. Such as sending numerous thoughtless e-mails to larger issues like purposely sending computer viruses.
  - Not snoop around in other people's computer files. Don't go looking through other people's computer files unless given permission.

Ten Commandments of Computer ethics

- Not use a computer to steal.
- Not use a computer to bear false witness. Don't spread rumors or change your email address so that the receiver of an email believes that it came from someone other than yourself.
- Not copy or use proprietary software for which you have not paid. Once you buy a software system, music CD or DVD you should not make copies of that information and distribute it to your friends.

Ten Commandments of Computer ethics

- Not use other people's computer resources without authorization or proper compensation. This means do not surf the internet or print off large amounts of paper for personal use during work hours.
- Not appropriate other people's intellectual output. Don't upload information and take credit for it such as music, images and text.

Ten Commandments of Computer ethics

- Think about the social consequences of the program you are writing or the system you are designing.

Lecture 1
Chapter 1

Objectives

- As you read 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?

Objectives (cont'd.)

- Why are organizations interested in fostering good business ethics?
- What approach can you take to ensure ethical decision making?
- What trends have increased the risk of using information technology in an unethical manner?

What is Ethics?

- Moral code
  - Set of rules
  - Establishes boundaries of generally accepted behaviour
  - Different rules often have contradictions
  - E.g. Caught friend cheating? Personal privacy?
- Morality
  - Social conventions about right and wrong
  - Widely shared
  - Form basis for an established consensus

What is Ethics? (cont'd.)

- 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 (fairness, generosity, Loyalty etc)
- Vices
  - Habits of unacceptable behavior (vanity, Greed, anger, envy etc)
- Virtues and vices define a personal value system
  - Scheme of moral values

Discussions

- Software Privacy?
- Respecting A women?
- Treating Rich and poor?
- Norms defined by religion?
- Lying?

The Importance of Integrity

- Integrity is a cornerstone of ethical behaviour
- 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

Discussions

- Is it ok to lie? (fir Kids? For adults)
- Is it acceptable to exaggerate your work experience on a résumé?
- Can you cut corners on a project to meet a tight deadline?
- To extend to all people the same respect and consideration that you expect to receive from others?
- Asking for over-time hours payments during budget constraints?

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

Discussions

- Morals & ethics of a teacher; Law for a teacher?
- Morals & ethics of a Student; Law for a student?

Ethics in the Business World

- Both the likelihood and the negative impact of inappropriate behaviour have increased
- Several trends have increased the likelihood of unethical behaviour:
  - Globalization creating complex work environments
  - Organizations challenged to maintain profits / revenue
  - Heightened vigilance by:
    - Employees
    - Shareholders
    - Regulatory agencies

Ethics in the Business World (cont'd.)

- Recent scandals in IT companies
  - Satyam Computer Services (India)
  - Hewlett Packard
  - Computer Associates International
  - IBM
  - Enron Accounting Scandel
- Not just executives, but even lower-level employees, can find themselves in the middle of an ethical dilemma

Discussions

- Moving operations to third world countries?
- Organizations are extremely challenged to maintain revenue and profits?
- Production of unsafe/ substandard products?

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

Microsoft's statement of values

Our Values

As a company, and as individuals, we value integrity, honesty, openness, personal excellence, constructive self-criticism, continual self-improvement, and mutual respect. We are committed to our customers and partners and have a passion for technology. We take on big challenges, and pride ourselves on seeing them through. We hold ourselves accountable to our customers, shareholders, partners, and employees by honoring our commitments, providing results, and striving for the highest quality.

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 non-profit institutions
    - Providing benefits for employees in excess of legal requirements
    - Choosing economic opportunities that might be more socially desirable than profitable

Gaining the Good Will of the Community (cont'd.)

- 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

Creating an Organization That Operates Consistently (cont'd.)

- 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 most 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

Fostering Good Business Practices (cont'd.)

- 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 & 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 ***respondent superior (let the Master answer)***
- 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/Compliance 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

Appointing a Corporate Ethics Officer (contd…)

- Corporate ethics/Compliance officer should provide
  - **Responsibility for compliance**: ensuring that ethical procedures are put into place and consistently adhered to throughout the organization
  - **Responsibility for creating and maintaining the ethics culture** that the highest level of corporate authority wishes to have
  - **Responsibility for being a key knowledge and contact person** on issues relating to corporate ethics and principles

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

Ethical Standards Set by Board of Directors

- In a for-profit organization, the board's primary objective is to oversee the organization's business activities and management for the benefit of all stakeholders, including shareholders, employees, customers, suppliers, and the community.

- In a nonprofit organization, the board reports to a different set of stakeholders, particularly the local community that the nonprofit serves.

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

Establishing a Corporate Code of Ethics (cont'd.)

- 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 Securities and Exchange Commission (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

Establishing a Corporate Code of Ethics (cont'd.)

- 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

Establishing a Corporate Code of Ethics (cont'd.)

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

Intel's five principles of conduct

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

In a social audit, an organization reviews how well it is meeting its ethical and social responsibility goals, and communicates its new goals for the upcoming year

Conducting Social Audits

2007 Goals	2007 Performance	Results
Audit 20% of our suppliers who may be at high risk for nonconformance to the EICC	We did not reach our 20% goal; challenges included industry-wide supplier classification and auditor training	Did not meet goal
Reduce greenhouse gas emissions per production unit by 30% from 2004 levels by 2010	Goal remains on track; absolute greenhouse gas emissions were down 6%	Met our goal
Reduce water usage per production unit below 2005 levels by 2010	Absolute water use was down 2%; usage was up 4% per chip	Did not meet goal
Recycle more than 70% of both chemical and solid waste generated from our worldwide facilities	In 2007, Intel recycled 89% of the solid waste and 87% of the chemical waste generated at our facilities worldwide	Met our goal
Empower students and teachers by donating 20,000 computers to schools in developing nations	Donated 27,000 full-featured PCs with Internet connectivity to more than 500 schools in 22 countries as part of our education donation program	Met our goal

Partial Intel 2007 Corporate Responsibility Report

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

Requiring Employees to Take Ethics Training (cont'd.)

- Critical that 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

- Only 43% of companies include ethical conduct in employee's performance appraisal
- Ethical criteria include:
  - Treating others fairly and with respect
  - Operating effectively in a multicultural environment
  - Accepting personal accountability
  - Continually developing themselves and others
  - Operating openly and honestly with all

The End

Lecture 2
Chapter 1

Objectives

- As you read 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?

Objectives (cont'd.)

- Why are organizations interested in fostering good business ethics?
- What approach can you take to ensure ethical decision making?
- What trends have increased the risk of using information technology in an unethical manner?

Creating an Ethical Work Environment

- 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

Creating an Ethical Work Environment (cont'd.)

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

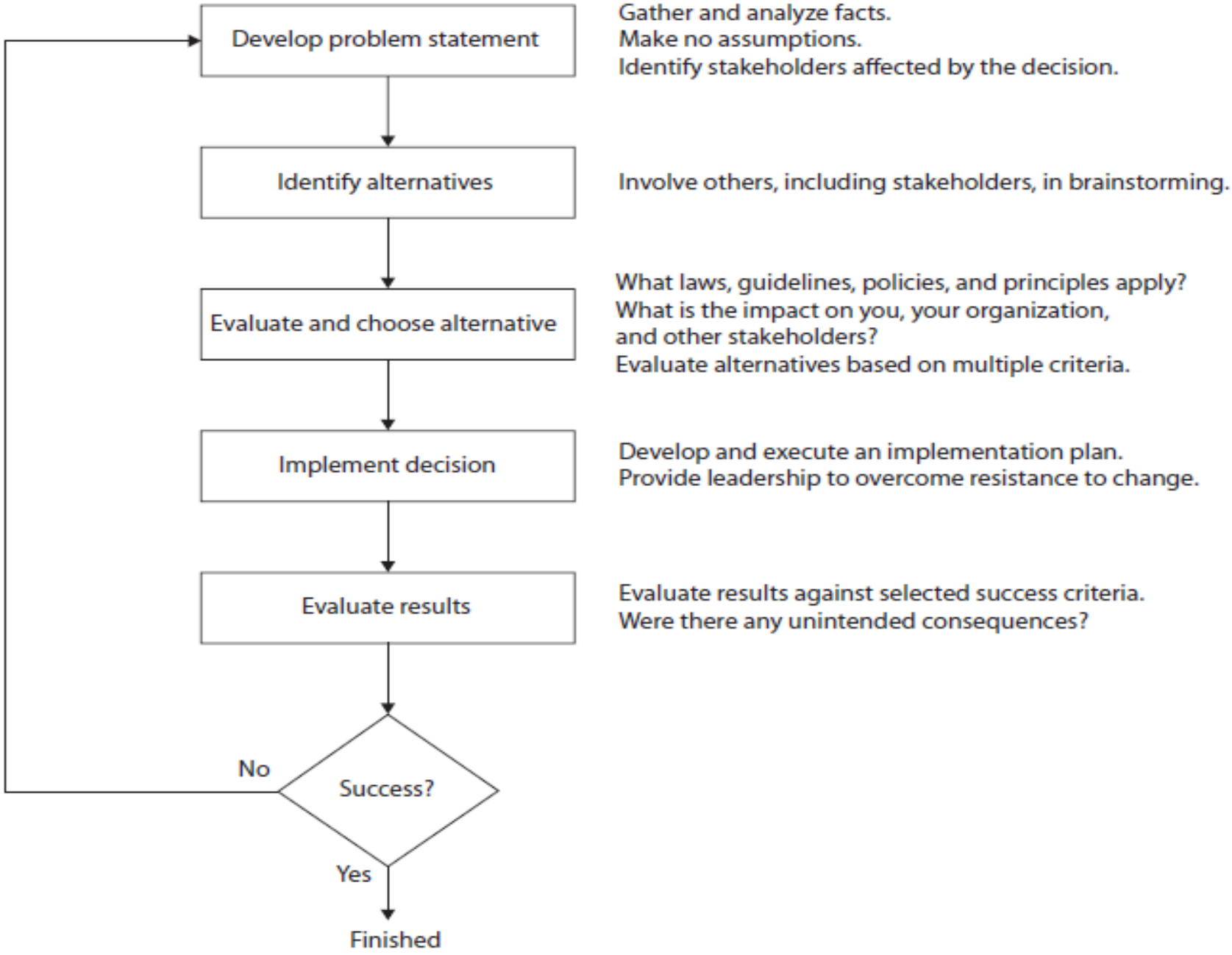

FIGURE 1-4 Decision-making process

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
- Gather & analyze facts
- Seek information and opinions from a variety of people
- No assumptions
- Identifying stakeholders

Develop a Problem Statement (cont'd.)

- 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

Evaluate, and Choose an Alternative

- Alternatives are evaluated on numerous criteria:
  - effectiveness at addressing the issue
  - the extent of risk associated with each alternative
  - Cost to implement
  - Time to implement

Decision Making

- Philosophers have developed many approaches to aid in ethical decision making
- provide a framework for decision makers to reflect on the acceptability of their actions and evaluate their moral judgments
- People must find the appropriate balance between all applicable laws, corporate principles, and moral guidelines to help them make decisions

Common Approaches to Ethical Decision Making

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
  - Focuses on how you should behave and think about relationships if you are concerned with your daily life in a community.
  - People guided by virtues to reach "right" decision
  - More effective than following set of principles/rules
  - Bravery etc.
- 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
  - effective education system, a safe and efficient transportation system,and accessible and affordable health care
- 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

Ethics in Information Technology (cont'd.)

- 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

Ethics in Information Technology (cont'd.)

- 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

Summary (cont'd.)

- 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

Summary (cont'd.)

- Four common approaches to ethical decision making
  - Virtue ethics approach
  - Utilitarian approach
  - Fairness approach
  - Common good approach

The End

Chapter 2
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?

Objectives (cont'd.)

- How do codes of ethics, professional organizations, certification, and licensing affect the ethical behavior of IT professionals?
- What are the key points of five different codes of ethics that provide guidance for IT professionals?

IT Professionals

- Profession is a calling **requiring specialized knowledge** and often **long intensive academic preparation.**

- Professionals:
  - Require advanced training and experience
  - Must exercise discretion and judgment in their work
  - Cannot standardize their work
  - Carry special rights and responsibilities

U.S. Code of Federal Regulations

- The person "employed in a professional capacity" as one who meets these four criteria:
  1. One's primary duties consist of the performance of work requiring knowledge of an advanced type in a field of science or learning customarily acquired by a prolonged course of specialized intellectual instruction and study or work.
  2. One's instruction, study, or work is original and creative in character in a recognized field of artistic endeavor, the result of which depends primarily on the invention, imagination, or talent of the employee.

U.S. Code of Federal Regulations

3. One's work requires the consistent exercise of discretion and judgment in its performance.
4. One's work is predominantly intellectual and varied in character, and the output or result cannot be standardized in relation to a given period of time.

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)

Are IT Workers Professionals? (cont'd.)

- Legal perspective
  - IT workers are not recognized as professionals
  - Not licensed by state or federal government
  - IT workers are not liable for malpractice

The Changing Professional Services Industry

- Although not legally classified as professionals, 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 (real-time work in progress)
  - Modularization (able to outsource modules)
  - Globalization (industry extremely competitive)
  - Commoditization (for low-end services)

Seven forces that are changing nature of professional services

- **Client Sophistication**

Clients are more aware of what they need from service providers, more willing to look outside their own organization to get the best possible services, and better able to drive a hard bargain to get the best possible services at the lowest possible cost.

- **Governance**

Major scandals and tougher laws enacted to avoid future scandals (e.g., Sarbanes-Oxley) have created an environment in which there is less trust and more oversight in client– service provider relationships.

Seven forces that are changing nature of professional services

- **Connectivity**

Clients and service providers have built their working relationships on the expectation that they can communicate easily and instantly around the globe through electronic teleconferences, audio conferences, e-mail, and wireless devices.

- **Transparency**

Clients expect to be able **to see work-in-progress** in real time, and they expect to be able to influence that work. No longer are clients willing to wait until the end product is complete before they weigh in with comments and feedback..

Seven forces that are changing nature of professional services

- **Modularization**

Clients are able to **break down their business processes** into the fundamental steps and decide which they will perform themselves and which they will outsource to service providers.

- **Globalization**

Clients are able to evaluate and choose among service providers around the globe, making the service provider industry extremely competitive.

Seven forces that are changing nature of professional services

- **Commoditization**

Clients look at the delivery of **low-end services** (e.g., staff augmentation to complete a project) as a commodity service for which price is the primary criterion for choosing a service provider. For the delivery of **high-end services** (e.g., development of an IT strategic plan), clients seek to form a partnership with their service providers.

Professional Relationships That Must Be Managed

- IT workers have many different relationships with:
  - Employers
  - Clients
  - Suppliers
  - Other professionals
  - IT users
  - Society at large

Relationships Between IT Workers and Employers

- **Employment offer includes:**
  - ✓ Job title
  - ✓ General performance expectations
  - ✓ Specific work responsibilities
  - ✓ Drug-testing requirements
  - ✓ Dress code Location of employment
  - ✓ Salary
  - ✓ work hours
  - ✓ company benefits
- **Company's policy and procedures manual includes:**
  - ➢ Protection of company secrets
  - ➢ Vacation policy
  - ➢ Time off for a funeral or an illness in the family
  - ➢ Tuition reimbursement
  - ➢ Use of company resources, including computers and networks

Relationships Between IT Workers and Employers

- 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
    - BSA hotline (1-888-NO-PIRACY),
    - "Know It, Report It, Reward It"

Relationships Between IT Workers and Employers (cont'd.)

TABLE 2-1 Members of Business Software Alliance (as of January 2009)

Adobe	Apple	Autodesk
Bentley Systems	Borland	CA
Cadence	Cisco Systems	CNC Software-Mastercam
Corel	CyberLink	Dassault Systemes SolidWorks Corporation
Dell	EMC	HP (Hewlett-Packard)
IBM	Intel	Intuit
McAfee	Microsoft	Mindjet
Minitab	Monotype Imaging	Quark
Quest	Rosetta Stone	SAP
Siemens	Sybase	Symantec

Relationships Between IT Workers and Employers (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
- It **includes**: design of new software code, hardware designs, business plans, the design of a user interface to a computer program, and manufacturing processes.
- **Examples** includes: the Colonel's secret recipe of 11 herbs and spices, the formula for Coke, and Intel's manufacturing process for the i7 quad core processing chip

Relationships Between IT Workers and Employers (cont'd.)

- IT workers must set an example and enforce policies regarding the ethical use of IT in: (cont'd)
  - **Whistle-blowing**
    - Employee attracts attention to a negligent, illegal, unethical, abusive, or dangerous act that threatens the public interest
    - Whistle-blowers often have special information based on their expertise or position within the offending organization.
- For example, an employee of a chip manufacturing company may know that the chemical process used to make the chips is dangerous to employees and the general public. A conscientious employee would call the problem to management's attention and try to correct it by working with appropriate resources within the company. But what if the employee's attempt to correct the problem through internal channels was thwarted or ignored? The employee could then consider becoming a whistle-blower and reporting the problem to people outside the company, including state or federal agencies that have jurisdiction. Obviously, such actions could have negative consequences on the employee's job, perhaps resulting in retaliation and firing.

Relationships Between IT Workers and Clients

- IT worker provides:
  - Hardware, software, or services at a certain cost and within a given time frame
- Relationship is usually documented in contractual terms:

✓ *who does what?*

✓ *when the work begins?*

✓ *how long it will take?*

✓ *how much the client pays and so on?*

- Client makes **decisions** about a project on the basis of **information, alternatives, and recommendations provided by the IT worker.**
- The responsibility for decision making is shared between client and IT worker

Relationships Between IT Workers and Clients (cont'd.)

- Ethical problems arise if a company recommends its own products and services to remedy problems they have detected
  - A company is unable to provide full and accurate reporting of a project's status
- Problems can also arise during a project if IT workers find themselves unable to provide full and accurate reporting of the project's status due to a lack of information, tools, or experience needed to perform an accurate assessment.
- finger-pointing and heated discussions about cost overruns, missed schedules, and technical incompetence can lead to charges of ***fraud***, ***misrepresentation***, and ***breach of contract***

Relationships Between IT Workers and Clients (cont'd.)

- Fraud
  - Crime of obtaining goods, services, or property through deception or trickery
  - Fraud is proven in court
  - Prosecutors must demonstrate the following elements:
    - The wrongdoer made a false representation of material fact.
    - The wrongdoer intended to deceive the innocent party.
    - The innocent party justifiably relied on the misrepresentation.
    - The innocent party was injured.

Relationships Between IT Workers and Clients (cont'd.)

- Misrepresentation
  - Misstatement or incomplete statement of material fact
  - Problem if causes entry into contract
- If the misrepresentation causes the other party to enter into a contract, that party may have the legal right to cancel the contract or seek reimbursement for damages.
- Breach of contract
  - One party fails to meet the terms of a contract
- Material breach of contract
- occurs when a party fails to perform certain express or implied obligations, which impairs or destroys the essence of the contract

Relationships Between IT Workers and Clients (cont'd.)

- There is no clear line between a **minor breach and a material breach**, determination is made on a case-by-case basis.
- "When there has been a material breach of contract, the non-breaching party can either:

(1) rescind the contract, seek restitution of any compensation paid under the contract to the breaching party, and be discharged from any further performance under the contract

(2) treat the contract as being in effect and sue the breaching party to recover damages

Relationships Between IT Workers and Clients (cont'd.)

- Consider the following frequent **causes of problems** in IT projects:
  - The customer changes the scope of the project or the system requirements.
  - Poor communication between customer and vendor leads to performance that does not meet expectations.
  - The vendor delivers a system that meets customer requirements, but a competitor comes out with a system that offers more advanced and useful features.
  - The customer fails to reveal information about legacy systems or databases that make the new system extremely difficult to implement.

Who is to blame in such circumstances?

Relationships Between IT Workers and Clients (cont'd.)

- IT projects are joint efforts in which vendors and customers work together
  - Difficult to assign blame

Relationships Between IT Workers and Suppliers

- IT workers deal with many different hardware, software, and service providers.
- Develop good working relationships with suppliers:
  - To encourage flow of useful information and ideas
  - By dealing fairly with them
  - By not making unreasonable demands
- Bribery
  - Providing money, property, or favours 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

Relationships Between IT Workers and Suppliers (cont'd.)

- Bribery (cont'd.)
  - At what point does a gift become a bribe?
  - No gift should be hidden
  - Perceptions of donor and recipient can differ

Relationships Between IT Workers and Suppliers (cont'd.)

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

Relationships Between IT Workers and Other Professionals

- Professionals owe each other adherence to a profession's code of conduct
- Professionals feel a degree of loyalty to the other members of their profession.
- Ethical problems among the IT profession
  - **Résumé inflation**
- which involves lying on a résumé and claiming competence in an IT skill that is in high demand
- Some studies have shown that around 30 percent of all job applicants exaggerate their accomplishments, while roughly 10 percent "seriously misrepresent" their backgrounds

Relationships Between IT Workers and Other Professionals

- Inappropriate sharing of corporate information

- ✓ Because of their roles, IT workers have access to corporate databases of private and confidential information about employees, customers, suppliers, new product plans, promotions, budgets, and so on
- ✓ It might be sold to other organizations or shared informally during work conversations with others who have no need to know

Relationships Between IT Workers and IT Users

- IT user: person using a hardware or software product
- IT workers: develop, install, service, and support the product
- IT workers' duties
  - Understand users' needs and capabilities
  - Deliver products and services that meet those needs
  - Establish environment that supports ethical behaviour:
    - 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

THE END

Chapter 2
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?

Objectives (cont'd.)

- How do codes of ethics, professional organizations, certification, and licensing affect the ethical behavior of IT professionals?
- What are the key tenets of five different codes of ethics that provide guidance for IT professionals?

Professional Codes of Ethics

- State the principles and core values that are essential to the work of an occupational group
- Practitioners in many professions subscribe to a code of ethics that governs their behavior
- 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

Professional Codes of Ethics (cont'd.)

- Benefits individual, profession, and society as a whole
  - Ethical decision making

Adherence to a professional code of ethics means that practitioners use a common set of core values and beliefs as a guideline for ethical decision making.

  - High standards of practice and ethical behavior

Adherence to a code of ethics reminds professionals of the responsibilities and duties that they may be tempted to compromise to meet the pressures of day-to-day business

Professional Codes of Ethics (cont'd.)

- Trust and respect from general public

✓ Public trust is built on the expectation that a professional will behave ethically

✓ adherence to a code of ethics enhances trust and respect for professionals and their profession

- Evaluation benchmark for self-assessment

✓ A code of ethics provides an evaluation benchmark that a professional can use as a means of self-assessment. Peers of the professional can also use the code for recognition or censure.

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)
  - Association of IT Professionals (AITP)
  - Institute of Electrical and Electronics Engineers Computer Society (IEEE-CS)
  - Project Management Institute (PMI)
  - SysAdmin, Audit, Network, Security (SANS) Institute

Certification

- Indicates that a professional possesses a particular set of skills, knowledge, or abilities in the opinion of a certifying organization
- Can also apply to products (the Wi-Fi CERTIFIED logo assures that the product has met rigorous interoperability testing to ensure that it will work with other Wi-Fi-certified products)
- Generally voluntary
- Employers view as benchmark of knowledge
- Opinions are divided on value of certification

Certification (cont'd.)

- Vendor certifications
  - Cisco, IBM, Microsoft, Sun, SAP, and Oracle
  - 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
  - Can take years to obtain experience
  - Training can be expensive
  - Workers are commonly recertified as newer technologies become available

Certification (cont'd.)

- Industry association certifications
  - Require a higher level of experience and a broader perspective than vendor certifications
  - 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

- Generally administered at the state level in the United States
- Requires that recipient pass a test
- Case for licensing IT workers
  - Encourages following highest standards of profession
  - Encourages practicing a code of ethics
  - Violators would be punished
- Without licensing, no requirements for heightened care and no concept of professional malpractice

Government Licensing (cont'd.)

- Issues with government licensing of IT workers
  - 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:
  - 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 behavior
  - Enable management to punish violators
- Policy components include:
  - Establishing guidelines for use of company software
  - Defining and limiting appropriate use of IT resources
  - Structuring information systems to protect data and information
  - Installing and maintaining a corporate firewall

Supporting the Ethical Practices of IT Users (cont'd.)

TABLE 2-5 Manager's checklist of items to consider when 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		

Supporting the Ethical Practices of IT Users (cont'd.)

TABLE 2-5 Manager's checklist of items to consider when establishing an IT usage policy (continued)

Question	Yes	No
Does the policy address the following issues? • Protection of the data privacy rights of employees, customers, suppliers, and others • Limits and control of access to proprietary company data and information • Use of unauthorized or pirated software • Employee monitoring, including e-mail, 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 e-mailing, 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, use of "hard-to-guess" passwords, and frequent changing of passwords • The use of the computer to intimidate, harass, or insult others through abusive language in e-mails 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?		

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 there
- IT professionals have many different relationships
  - Each with its own ethical issues and potential problems

Summary (cont'd.)

- 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 behavior
  - 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

Summary (cont'd.)

- IT-related professional organizations have developed a code of ethics
- These codes:
  - Outline what the organization aspires to become
  - List rules and principles for members
  - Include a commitment to continuing education for those who practice the profession

THE END

CHAPTER 3
COMPUTER AND INTERNET CRIME

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)

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

Distributed Denial-of-Service (DDoS) Attacks

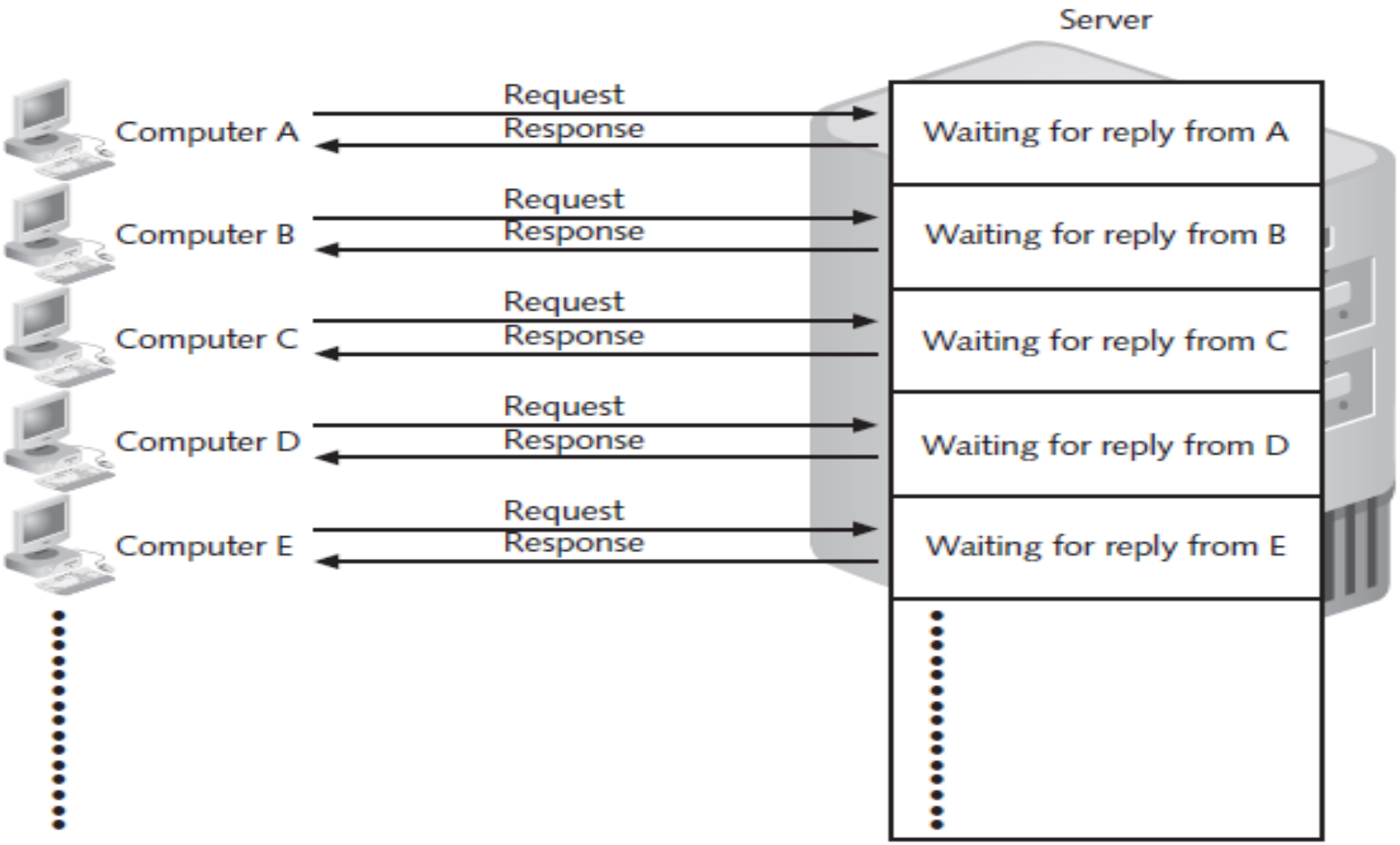

FIGURE 3-2 Distributed denial-of-service attack

Source Line: Course Technology/Cengage Learning.

Distributed Denial-of-Service (DDoS) Attacks

- The software to initiate a denial-of-service attack is simple to use, and over 55 DDoS tools are readily available at a variety of hacker sites.
- A tiny program is downloaded surreptitiously from the attacker's computer to dozens, hundreds, or even thousands of computers all over the world.
- The term botnet is used to describe a large group of such computers, which are controlled from one or more remote locations by hackers, without the knowledge or consent of their owners.

Distributed Denial-of-Service (DDoS) Attacks

- The collective processing capacity of some botnets exceeds that of the world's most powerful supercomputers.
- Based on a command by the attacker or at a preset time, the botnet computers (called zombies) go into action, each sending a simple request for access to the target site again and again—dozens of times per second.
- The target computers are so overwhelmed by requests for service that legitimate users are unable to "get through" to the target computer.

Distributed Denial-of-Service (DDoS) Attacks

- Banks and other e-commerce Web sites are frequent targets of botnets. Both the Bank of America and Chase banks were hit with a DDoS attack in the fall of 2012.
- Botnets are also frequently used to distribute spam and malicious code.
- The Grum botnet was first detected in 2008 and operated until 2012 when it was brought down by cybercrime fighters.
- Grum infected several hundred thousand computers around the world.

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
- Attacker can:
  - execute files
  - access logs
  - monitor user activity
  - change the computer's configuration

Rootkits

- Blended threat, consisting :
- **Dropper**: gets the rootkit installation started and can be activated by clicking on a link to a malicious Web site in an e-mail or opening an infected .pdf file. launches the loader program and then deletes itself
- **Loader**: The loader loads the rootkit into memory
- **Rootkit**: at that point the computer has been compromised.

Rootkits

Here are some symptoms of rootkit infections:

- The computer locks up or fails to respond to input from the keyboard or mouse.
- The screen saver changes without any action on the part of the user.
- The taskbar disappears.
- Network activities function extremely slowly.

Rootkits

- When it is determined that a computer has been infected with a rootkit, there is little to do but reformat the disk; reinstall the operating system and all applications; and reconfigure the user's settings, such as mapped drives.
- This can take hours, and the user may be left with a basic working machine, but all locally held data and settings may be lost.

Rootkits

- A recent rootkit, labeled the “2012 rootkit virus,” is a nasty piece of malware that deletes information from a computer and makes it impossible to run some applications, such as Microsoft Word.
- The longer the rootkit is present, the more damage it causes.
- The virus asks users to install what appears to be a legitimate update to their antivirus software or some other application. By the time the user sees the prompt to install the software, it is too late, the computer has already been infected by the rootkit

Phishing

- **Phishing** is the act of fraudulently using email to try to get the recipient to reveal personal data.
- In a phishing scam, con artists send legitimate-looking emails urging the recipient to take action to avoid a negative consequence or to receive a reward.
- The requested action may involve clicking on a link to a Web site or opening an email attachment.
- These emails, such as the one shown in Figure 3-3, lead consumers to counterfeit Web sites designed to trick them into divulging personal data.

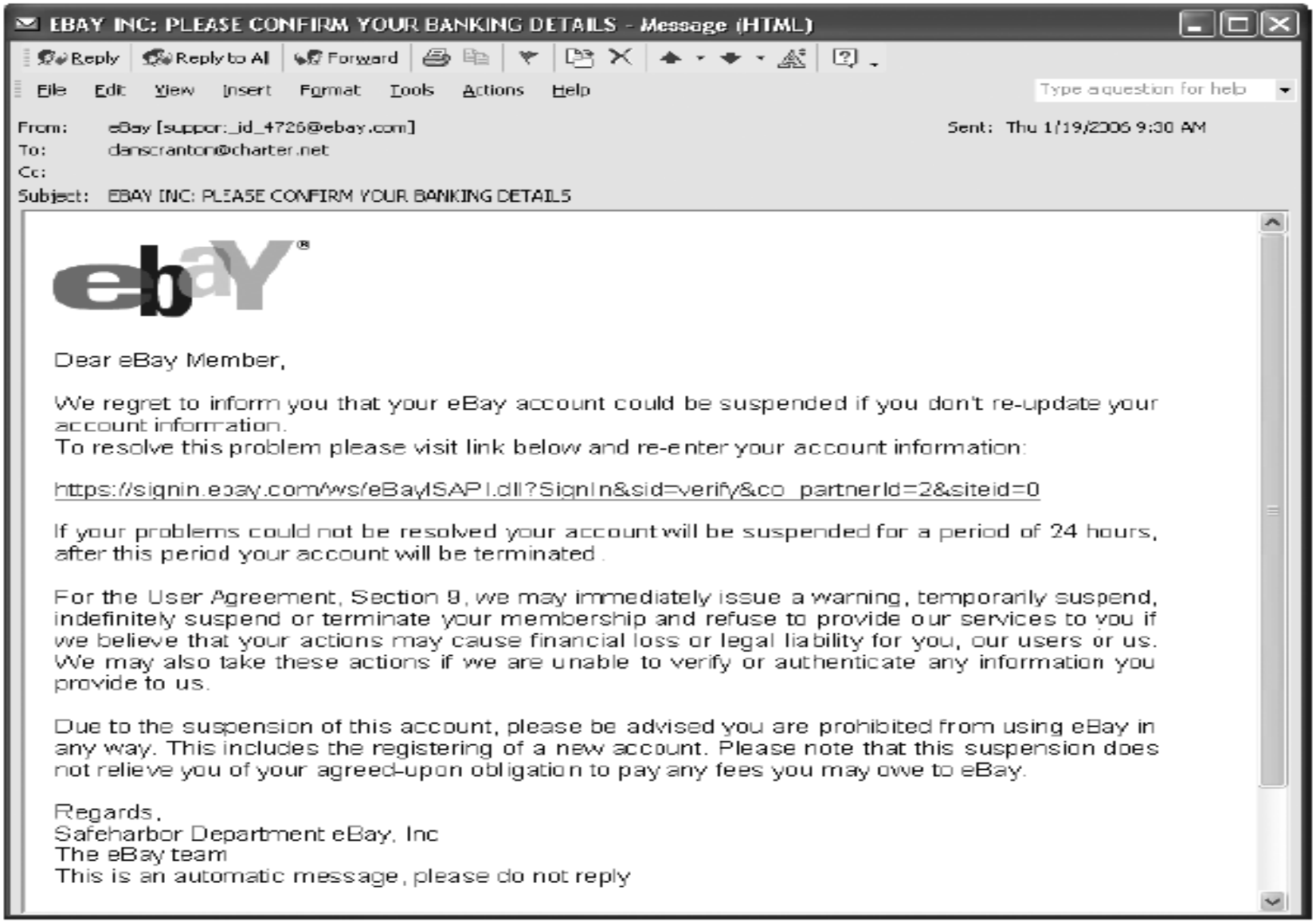

FIGURE 3-3 Example of phishing

Source Line: Course Technology/Cengage Learning.

Phishing

- Savvy users often become suspicious and refuse to enter data into the fake Web sites; however, sometimes just accessing the Web site can trigger an automatic and unnoticeable download of malicious software to a computer.
- Citibank, eBay, and PayPal are among the Web sites that phishers spoof most frequently. It is estimated that .03 percent of all emails sent in October 2012 were phishing attacks.

Phishing

Spear Phishing

- is a variation of phishing in which the phisher sends fraudulent emails to a certain organization's employees.
- It is known as spear-phishing because the attack is much more precise and narrow, like the tip of a spear.
- The phony emails are designed to look like they came from high-level executives within the organization.

Phishing

- Employees are directed to a fake Web site and then asked to enter personal information, such as name, Social Security number, and network passwords.
- Botnets have become the primary means for distributing phishing scams.
- Strategic Forecasting (commonly referred to as Stratfor) is an intelligence analysis firm whose clients include the U.S. Army, the Department of Defense, and military contractor Lockheed Martin.

Phishing

- A hacker group broke into the firm's network and stole information on thousands of email accounts.
- This information was used to initiate spear-phishing attacks on employees of the firm's clients.
- The emails, which were designed to look as if they came from Stratfor, directed recipients to a Web site that looked like the Stratfor Web site and instructed them to enter private information.
- In addition, the emails were laced with malware and other harmful attachments.

Phishing

Smishing

- **Smishing** is another variation of phishing that involves the use of Short Message Service (SMS) texting.
- a smishing scam, people receive a legitimate-looking text message on their phone telling them to call a specific phone number or to log on to a Web site.
- This is often done under the guise that there is a problem with their bank account or credit card that requires immediate attention.

Phishing

- However, the phone number or Web site is phony and is used to trick unsuspecting victims into providing personal information such as a bank account number, personal identification number, or credit card number.
- This information can be used to steal money from victims' bank accounts, charge purchases on their credit cards, or open new accounts.

Phishing

- In some cases, if victims log on to a Web site, malicious software is downloaded onto their phones, providing criminals with access to information stored on the phones.
- The number of smishing scams increases around the holidays as people use their cell phones to make online purchases.

Phishing

- **Vishing** is similar to smishing except that the victims receive a voice mail telling them to call a phone number or access a Web site.
- Here are two examples of smishing crimes:

1) Account holders at a credit union were sent a text about an account problem and were told to call a phone number provided in the text.

- If they did so, they were asked to provide personal information that allowed criminals to steal funds from their accounts within 10 minutes of the phone call

Phishing

2) Bank customers received a text stating that it was necessary to reactivate their automated teller machine (ATM) card.

- Those who called the phone number in the text were asked to provide their ATM card number, PIN, and expiration date. Thousands of victims had money stolen from their accounts.

Phishing

- Financial institutions, credit card companies, and other organizations whose customers may be targeted by criminals in this manner need to be on the alert for phishing, smishing, and vishing scams.
- They must be prepared to act quickly and decisively without alarming their customers if such a scam is detected.
- Recommended action steps for institutions and organizations include the following

Phishing

- Companies should educate their customers about the dangers of phishing, smishing, and vishing through letters, recorded messages for those calling into the company's call center, and articles on the company's Web site.
- Call center service employees should be trained to detect customer complaints that indicate a scam is being perpetrated. They should attempt to capture key pieces of information, such as the callback number the customer was directed to use, details of the phone message or text message, and the type of information requested.

Phishing

- Customers should be notified immediately if a scam occurs. This can be done via a recorded message for customers phoning the call center, working with local media to place a news article in papers serving the area of the attack, placing a banner on the institution's Web page, and even displaying posters in bank drive-through and lobby areas.
- If it is determined that the calls are originating from within the United States, companies should report the scam to the Federal Bureau of Investigation (FBI).

Phishing

- Institutions can also try to notify the telecommunications carrier for the particular phone number that victims are requested to call, to request that they shut down that number.

Spam

- **Email Spam**: Abuse of email systems to send unsolicited email to large numbers of people
- Spam is also an extremely inexpensive method of marketing used by many legitimate organizations
  - 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

Spam (cont'd.)

- Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA)
  - Software generates tests that humans can pass but computer programs cannot

Types of Perpetrators

- People who launch exploits(various computer attacks)
- 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

Types of Perpetrators (cont'd.)

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

- Test limitations of systems out of intellectual curiosity
- have at least a basic understanding of information systems and security features
  - Some smart and talented
  - Others inept; termed "**lamers**" or "**script kiddies**"

- Twitter Hacking:
  - Force victims to join his Twitter follow list automatically
  - Vint Cerf: used it for spamming
- Hacking that borders on cyber-terrorism (Chinese hackers have repeatedly hacked into systems to intercept e-mails between U.S. and UK government officials)
- hacker conventions (such as DEFCON, an annual gathering in Las Vegas

Crackers

- Crackers
  - A form of hacking
  - Clearly criminal activity
- Crackers break into other people's networks and systems to cause harm
- defacing Web pages
- crashing computers
- spreading harmful programs or hateful messages
- writing scripts and automated programs that let other people do the same things

Malicious Insiders

- Major security concern for companies
- An ever present and extremely dangerous adversary
- 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
- *typical employee who commits fraud has many years with the company, is an authorized user, is in a nontechnical position, has no record of being a problem employee, uses legitimate computer commands to commit the fraud, and does so mostly during business hours*

Malicious Insiders

- Extremely difficult to detect or stop
  - Authorized to access the very systems they abuse
- Negligent insiders have potential to cause damage
- steps organizations can take to reduce the potential for attacks from insiders
  - Perform a thorough background check
  - Establish an expectation of regular and ongoing psychological and drug testing
  - Carefully limit the number of people who can perform sensitive operations
  - Define job roles and procedures
  - Periodically rotate employees in sensitive positions
  - Immediately revoke all rights and privileges required to perform old job responsibilities
  - Implement an ongoing audit process

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
  - financial reports, trade journals, public filings, and printed interviews with company officials
- Industrial espionage
  - Uses illegal means
  - Obtains information not available to the public
- wiretap on the phones of key company officials, bug a conference room, or break into a research and development facility to steal confidential test results

Industrial Spies

- Industrial espionage can involve the theft of new product designs, production data, marketing information, or new software source code.
- Industrial spy:
  - steal trade secrets
  - Avoids taking risks that would expose his employer, as the employer's reputation would be considerably damaged if the espionage were discovered

Cybercriminals

- Hack into corporate computers to steal
- motivated by the potential for monetary gain
- Engage in all forms of computer fraud
- **Charge-backs**: disputed transactions
- It includes all forms of computer fraud: stealing and reselling credit card numbers, personal identities, and cell phone IDs

Cybercriminals

- 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

Cybercriminals (cont'd.)

- 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
  - a combination of the words hacking and activism
- 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
  - Specific targets might include telephone-switching systems, an electric power grid that serves major portions of a geographic region, or an air traffic control center that ensures airplanes can take off or land safely

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

Summary (cont'd.)

- Perpetrators include:
  - Hackers
  - Crackers
  - Malicious insider
  - Industrial spies
  - Cybercriminals
  - Hacktivist
  - Cyberterrorists

THE END