



Computer Ethics & Society

Chapter # 1

Overview of Ethics

ETHICS IN INFORMATION TECHNOLOGY BY GEORGE W. REYNOLDS

Prepared by: Shahid Hussain

What is Ethics?

- Each society forms a set of rules that establishes the boundaries of generally accepted behavior. These rules are often expressed in statements about how people should behave, and they fit together to form the *moral code* by which a society lives.
- The term *morality* refers to social conventions about right and wrong those are so widely shared that they become the basis for an established consensus.



Definition of Ethics & other terms

- **Ethics** is a set of beliefs about right and wrong behavior within a society.
- **Ethical behavior** conforms to generally accepted norms—many of which are almost universal.
- **Virtues** are habits that incline people to do what is acceptable.
- **Vices** are habits of unacceptable behavior.



The Difference Between Morals, Ethics, and Laws

- **Morals** are one's personal beliefs about right and wrong.
- The term **ethics** describes standards or codes of behavior expected of an individual by a group (nation, organization, profession) to which an individual belongs.
- **Law** is a system of rules that tells us what we can and cannot do. Laws are enforced by a set of institutions (the police, courts, law-making bodies).
- **Legal acts** are acts that conform to the law. Moral acts conform to what an individual believes to be the right thing to do.



ETHICS IN THE BUSINESS WORLD

- Ethics has risen to the top of the business agenda because the risks associated with inappropriate behavior have increased, both in their likelihood and in their potential negative impact.



Why Fostering Good Business Ethics Is Important

- Organizations have at least five good reasons for promoting a work environment in which employees are encouraged to act ethically when making business decisions:
 1. Gaining the good will of the community
 2. Creating an organization that operates consistently
 3. Fostering good business practices
 4. Protecting the organization and its employees from legal action
 5. Avoiding unfavorable publicity



Characteristics of a successful ethical program

The Ethics Resource Center has defined the following characteristics of a successful ethics program:

1. Employees are willing to seek advice about ethics issues.
2. Employees feel prepared to handle situations that could lead to misconduct.
3. Employees are rewarded for ethical behavior.
4. The organization does not reward success obtained through questionable means.
5. Employees feel positively about their company.

Improving Corporate Ethics

- The risk of unethical behavior is increasing, so the improvement of business ethics is becoming more important. The following sections explain some of the actions corporations can take to improve business ethics.
 - 1) Appointing a Corporate Ethics Officer
 - 2) Ethical Standards Set by Board of Directors
 - 3) Establishing a Corporate Code of Ethics
 - 4) Conducting Social Audits
 - 5) Requiring Employees to Take Ethics Training
 - 6) Including Ethical Criteria in Employee Appraisals

Creating an Ethical Work Environment

TABLE 1-4 A 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?		

Including Ethical Considerations in Decision Making

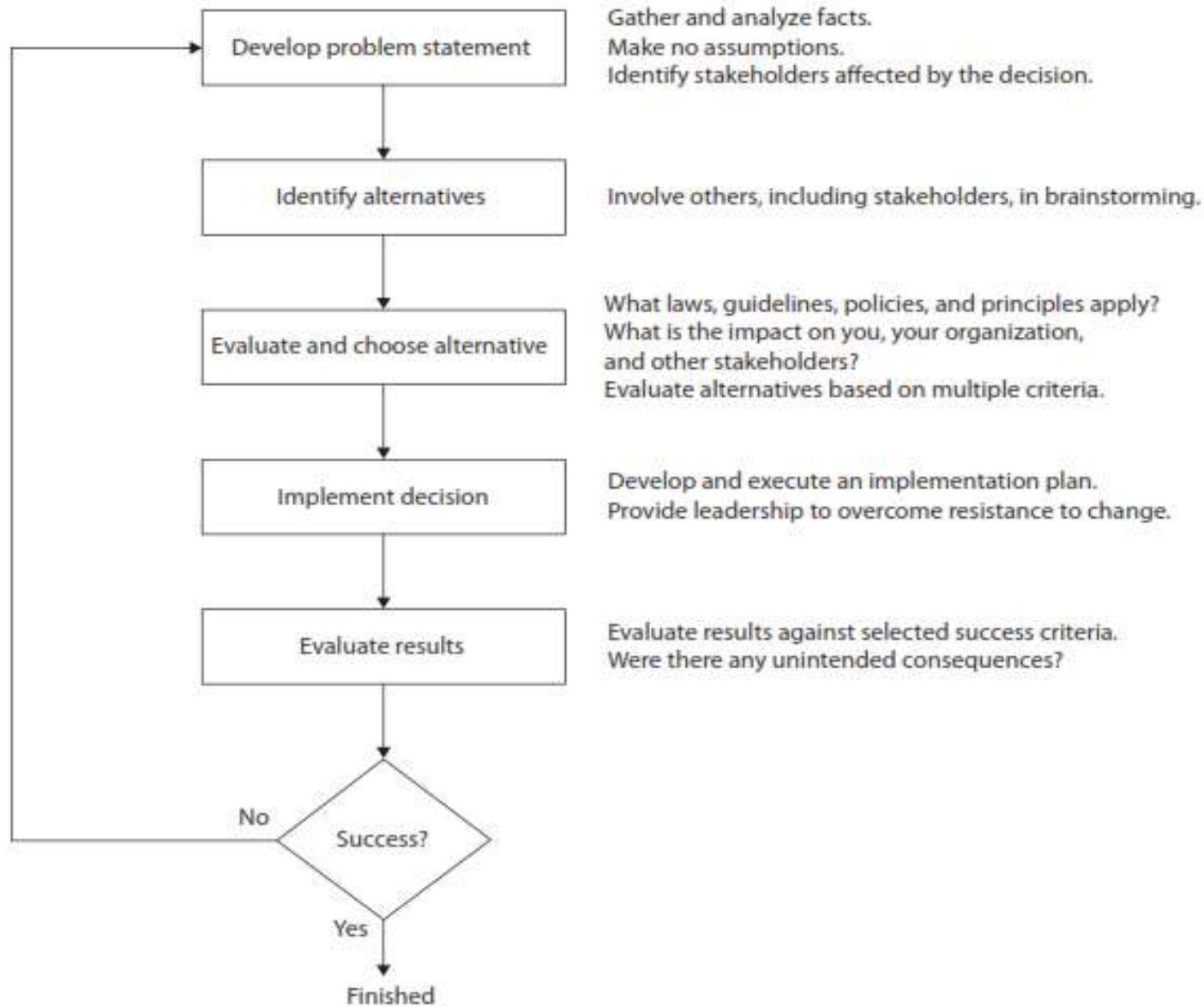


FIGURE 1-4 Decision-making process

Four common approaches to ethical decision making

- **Virtue Ethics Approach**

- The virtue ethics approach to decision making focuses on how you should behave and think about relationships if you are concerned with your daily life in a community.

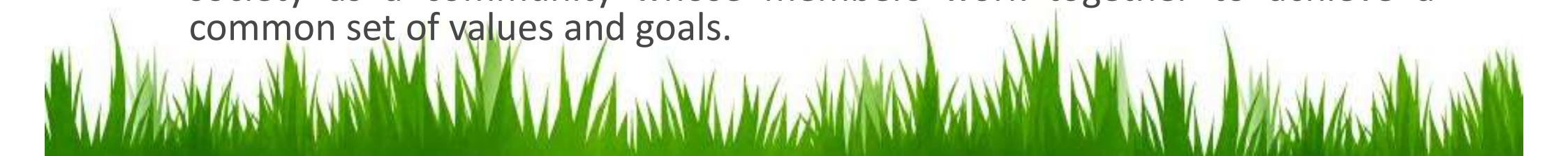
- **Utilitarian Approach**

- The utilitarian approach to ethical decision making states that you should choose the action or policy that has the best overall consequences for all people who are directly or indirectly affected.

- **Fairness Approach**


- The fairness approach focuses on how fairly actions and policies distribute benefits and burdens among people affected by the decision. The guiding principle of this approach is to treat all people the same.

- **Common Good Approach**

- The common good approach to decision making is based on a vision of society as a community whose members work together to achieve a common set of values and goals.
- 

ETHICS IN INFORMATION TECHNOLOGY

Here are some examples that raise public concern about the ethical use of information technology:

- Many employees might have their e-mail and Internet access monitored while at work, as employers struggle to balance their need to manage important company assets and work time with employees' desire for privacy and self-direction.
 - Millions of people have downloaded music and movies at no charge and in apparent violation of copyright laws at tremendous expense to the owners of those copyrights.
 - Organizations contact millions of people worldwide through unsolicited e-mail (spam) as an extremely low-cost marketing approach.
 - Hackers break into databases of financial and retail institutions to steal customer information, and then use it to commit identity theft—opening new accounts and charging purchases to unsuspecting victims.
 - Students around the world have been caught downloading material from the Web and plagiarizing content for their term papers.
 - Web sites plant cookies or spyware on visitors' hard drives to track their online purchases and activities.
- 



Question & Answer Session





Computer Ethics & Society

Chapter # 2

Ethics for IT workers & IT Users

ETHICS IN INFORMATION TECHNOLOGY BY GEORGE W. REYNOLDS

Prepared by: Shahid Hussain

Are IT workers professionals

- Many business workers have duties, backgrounds, and training that qualify them to be classified as professionals, including marketing analysts, financial consultants, and IT specialists.
- A partial list of IT specialists includes programmers, systems analysts, software engineers, database administrators, local area network (LAN) administrators, and chief information officers (CIOs).



Relationships Between IT Workers and IT Users

- The term IT user distinguishes the person who uses a hardware or software product from the IT workers who develop, install, service, and support the product.
- IT users need the product to deliver organizational benefits or to increase their productivity.
- IT workers have a duty to understand a user's needs and capabilities and to deliver products and services that best meet those needs.



Some Important Terminologies

- **Trade Secret** is information, generally unknown to the public, that has economic value and company has taken strong measures to keep confidential.
- **Whistle Blowing** is an effort by an employee to attract attention to a negligent, illegal, unethical, abusive, or dangerous act by a company that threatens the public interest.
- **Fraud** is the crime of obtaining goods, services, or property through deception or trickery.
- **Misrepresentation** is the misstatement or incomplete statement of a material fact.
- **Breach of contract** occurs when one party fails to meet the terms of a contract.
- **Bribery** involves providing money, property, or favors to someone in business or government to obtain a business advantage.

Professional Codes of Ethics

A professional code of ethics states the principles and core values that are essential to the work of a particular occupational group and helps promoting:

- **Ethical decision making**
- **High standards of practice and ethical behavior**
- **Trust and respect from the general public**
- **Evaluation benchmark**



Common Ethical Issues for IT Users

- **Software Piracy**

Sometimes IT users are the ones who commit software piracy. A common violation occurs when employees copy software from their work computers for use at home.

- **Inappropriate Use of Computing Resources**

Some employees use their computers to surf popular Web sites that have nothing to do with their jobs, participate in chat rooms, view pornographic sites, and play computer games.

- **Inappropriate Sharing of Information**

Some IT users can share secret and confidential information with an unauthorized party.



Supporting the Ethical Practices of IT Users

- Establishing Guidelines for Use of Company Software
- Defining and Limiting the Appropriate Use of IT Resources
- Structuring Information Systems to Protect Data and Information
- Installing and Maintaining a Corporate Firewall





- THANK YOU





Computer Ethics & Society

Chapter # 3

COMPUTER AND INTERNET CRIME

ETHICS IN INFORMATION TECHNOLOGY BY GEORGE W. REYNOLDS

Prepared by: Shahid Hussain

Overview

- The security of information technology used in business is of utmost importance.
- Confidential business data and private customer and employee information must be safeguarded, and systems must be protected against malicious acts of theft or disruption.
- Although the necessity of security is obvious, it must often be balanced against other business needs and issues.



Types of Exploits

- ***Virus*** is a piece of programming code, usually disguised as something else, which causes a computer to behave in an unexpected and usually undesirable manner.
- ***Worm*** is a harmful program that resides in the active memory of the computer and duplicates itself. Worms differ from viruses in that they can propagate without human intervention.
- ***Trojan Horse*** is a program in which malicious code is hidden inside a seemingly harmless program.
- ***Botnet*** is a large group of computers controlled from one or more remote locations by hackers, without the knowledge or consent of their owners. Botnets are frequently used to distribute spam and malicious code.

Types of Exploits (Contd.....)

- ***Distributed Denial-of-Service (DDoS) Attacks*** is one in which a malicious hacker takes over computers on the Internet and causes them to flood a target site with demands for data and other small tasks.
- ***Rootkit*** is a set of programs that enables its user to gain administrator level access to a computer without the end user's consent or knowledge.
- ***Spam*** E-mail spam is the abuse of e-mail systems to send unsolicited e-mail to large numbers of people. Most spam is a form of low-cost commercial advertising.
- ***Phishing*** is the act of using e-mail fraudulently to try to get the recipient to reveal personal data.
- ***Spear-phishing*** is a variation of phishing in which the phisher sends fraudulent e-mails to a certain organization's employees.

Types of Perpetrators

TABLE 3-3 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

IMPLEMENTING TRUSTWORTHY COMPUTING

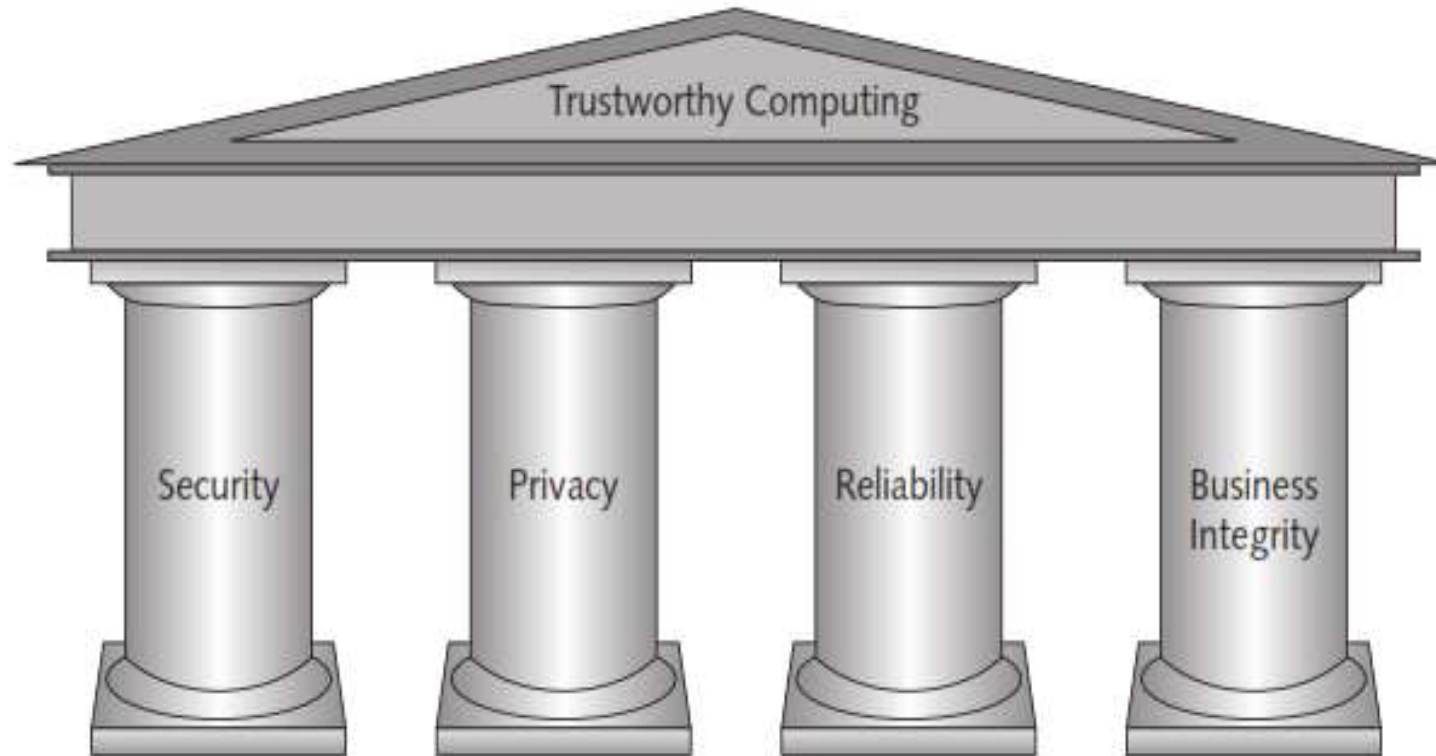


FIGURE 3-3 Microsoft's Four Pillars of Trustworthy Computing



Contd.....

TABLE 3-5 Actions taken by Microsoft to support trustworthy computing

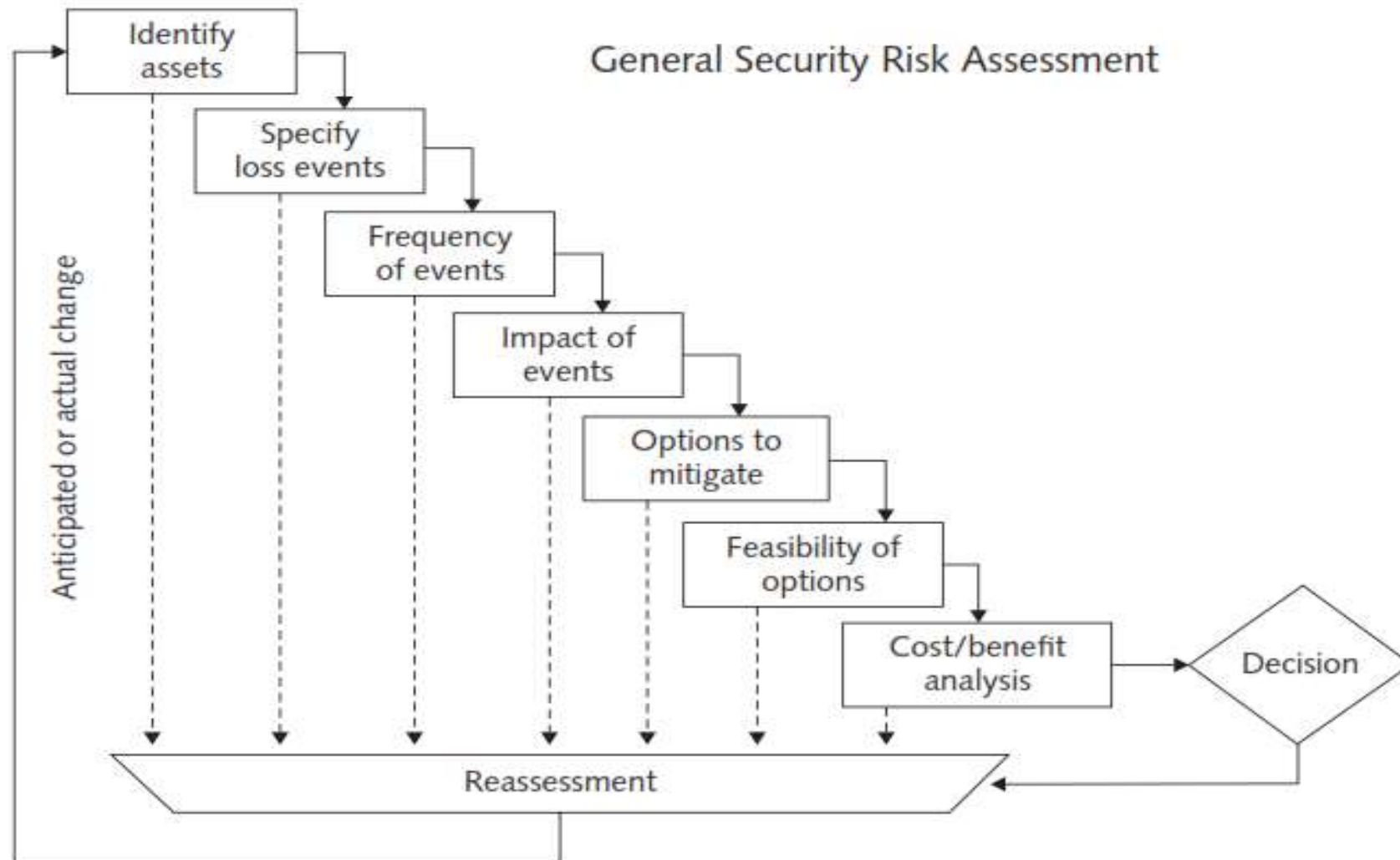
Pillar	Actions taken by Microsoft to support trustworthy computing
Security	<p>Invest in the expertise and technology required to create a trustworthy environment.</p> <p>Work with law enforcement agencies, industry experts, academia, and private sectors to create and enforce secure computing.</p> <p>Develop trust by educating consumers on secure computing.</p>
Privacy	<p>Make privacy a priority in the design, development, and testing of products.</p> <p>Contribute to standards and policies created by industry organizations and government.</p> <p>Provide users with a sense of control over their personal information.</p>
Reliability	<p>Build systems so that (1) they continue to provide service in the face of internal or external disruptions; (2) in the event of a disruption, they can be easily restored to a previously known state with no data loss; (3) they provide accurate and timely service whenever needed; (4) required changes and upgrades do not disrupt them; (5) on release, they contain minimal software bugs; and (6) they work as expected or promised.</p>
Business integrity	<p>Be responsive—take responsibility for problems and take action to correct them.</p> <p>Be transparent—be open in dealings with customers, keep motives clear, keep promises, and make sure customers know where they stand in dealing with the company.</p>

Risk Assessment

- A risk assessment is the process of assessing security-related risks to an organization's computers and networks from both internal and external threats.
- The goal of risk assessment is to identify which investments of time and resources will best protect the organization from its most likely and serious threats.



Risk Assessment Process



Source: General Security Risk Assessment Guideline, ASIS International, www.asisonline.org/guidelines/guidelinesgsra.pdf.

FIGURE 3-4 General Security Risk Assessment

Establishing a Security Policy

- A security policy defines an organization's security requirements, as well as the controls and sanctions needed to meet those requirements.
- A good security policy delineates responsibilities and the behavior expected of members of the organization.
- A security policy out-lines what needs to be done but not how to do it.
- The details of how to accomplish the goals of the policy are provided in separate documents and procedure guidelines.

Educating Employees, Contractors, and Part-Time Workers

Employees, contractors, and part-time workers must be educated about the importance of security so that they will be motivated to understand and follow the security policies.

For example, users must help protect an organization's information systems and data by doing the following:

- Guarding their passwords to protect against unauthorized access to their accounts
- Prohibiting others from using their passwords
- Applying strict access controls (file and directory permissions) to protect data from disclosure or destruction
- Reporting all unusual activity to the organization's IT security group

Prevention from threats

- *Installing a Corporate Firewall*
- *Intrusion Prevention Systems*
- *Installing Antivirus Software on Personal Computers*
- *Implementing Safeguards against Attacks by Malicious Insiders*
- *Conducting Periodic IT Security Audits*

Detection

- Even when preventive measures are implemented, no organization is completely secure from a determined attack.
- Thus, organizations should implement detection systems to catch intruders in the act.
- Organizations often employ an intrusion detection system to minimize the impact of intruders.
- An **intrusion detection system** is software and/or hardware that monitors system and network resources and activities, and notifies network security personnel when it identifies possible intrusions from outside the organization or misuse from within the organization.





Question & Answer Session





Computer Ethics & Society


Chapter # 4

Privacy

ETHICS IN INFORMATION TECHNOLOGY BY GEORGE W. REYNOLDS

Prepared by: Shahid Hussain

Introduction

- The use of information technology in business requires balancing the needs of those who use the information that is collected against the rights and desires of the people whose information is being used.
 - On the one hand, information about people is gathered, stored, analyzed, and reported because organizations can use it to make better decisions.
 - Some of these decisions, including whether or not to hire a job candidate, approve a loan, or offer a scholarship, can profoundly affect people's lives.
 - In addition, the global marketplace and intensified competition have increased the importance of knowing consumers' purchasing habits and financial condition.
 - Companies use this information to target marketing efforts to consumers who are most likely to buy their products and services.
 - Organizations also need basic information about customers to serve them better. It is hard to imagine an organization having productive relationships with its customers without having data about them.
 - Thus, organizations want systems that collect and store key data from every interaction they have with a customer.
- 

Information Privacy

Information privacy is the combination of

- communications privacy (the ability to communicate with others without those communications being monitored by other persons or organizations) and
- data privacy (the 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).



Data & Information Privacy Guidelines

Principle	Guideline
Collection limitation	Limit the collection of personal data; all such data must be obtained lawfully and fairly with the subject's consent and knowledge
Data quality	Personal data should be accurate, complete, current, and relevant to the purpose for which it is used
Purpose specification	The purpose for which personal data is collected should be specified and should not be changed
Use limitation	Personal data should not be used beyond the specified purpose without a person's consent or by authority of law
Security safeguards	Personal data should be protected against unauthorized access, modification, or disclosure
Openness principle	Data policies should exist, and a data controller should be identified
Individual participation	People should have the right to review their data, to challenge its correctness, and to have incorrect data changed
Accountability	A data controller should be responsible for ensuring that the above principles are met



KEY PRIVACY ISSUES

1. Identity Theft

Identity theft occurs when someone steals key pieces of personal information to impersonate a person. This information may include such data as name, address, date of birth, Social Security number, passport number, driver's license number, and mother's maiden name.

Four approaches are frequently used by identity thieves to capture the personal data of their victims:

- (1) Create a data breach to steal hundreds, thousands, or even millions of personal records;
- (2) Purchase personal data from criminals;
- (3) Use phishing to entice users to willingly give up personal data; and
- (4) Install spyware capable of capturing the keystrokes of victims.




2. Consumer Profiling

- Companies openly collect personal information about Internet users when they register at Web sites, complete surveys, fill out forms, or enter contests online.
- Many companies also obtain information about Web surfers through the use of cookies, text files that a Web site can download to visitors' hard drives so that it can identify visitors on subsequent visits.
- Companies also use tracking software to allow their Web sites to analyze browsing habits and deduce personal interests and preferences.



Contd.....

3. Treating Consumer Data Responsibly

- When dealing with consumer data, strong measures are required to avoid customer relationship problems.
 - The most widely accepted approach to treating consumer data responsibly is for a company to adopt the Fair Information Practices and the privacy guidelines.
 - Under these guidelines, an organization collects only personal information that is necessary to deliver its product or service.
 - The company ensures that the information is carefully protected and accessible only by those with a need to know, and that consumers can review their own data and make corrections.
 - The company informs customers if it intends to use customer information for research or marketing, and it provides a means for them to opt out.
- 

Contd.....

4. Workplace Monitoring

- Many organizations have developed a policy on the use of IT in the workplace in order to protect against employee abuses that reduce worker productivity or expose the employer to harassment lawsuits.

5. Advanced Surveillance Technology

- A number of advances in information technology—such as surveillance cameras, facial recognition software, and satellite-based systems that can pinpoint a person’s physical location—provide exciting new data-gathering capabilities.
- However, these advances can also diminish individual privacy and complicate the issue of how much information should be captured about people’s private lives.
- Camera Surveillance, Facial recognition systems and GPS chips are some of the latest and advanced surveillance technologies used in this respect.

Safeguarding your identity data

TABLE 4-3 Recommendations for safeguarding your identity data

Recommendation	Explanation
Completely and irrevocably destroy digital identity data on used equipment	As it is possible to undelete files and recover data, take necessary actions to ensure that all data is destroyed when you dispose of used computers and data storage devices; consider the use of special software, such as Shred XP
Shred everything	Identity thieves are not above “dumpster diving”—going through your garbage to find financial statements and bills in order to obtain confidential personal information
Require retailers to request a photo ID when accepting your credit card	Writing “Request Photo ID” on the back of your credit cards should prompt retailers to request a photo ID before accepting your card
Beware shoulder surfing	Ensure that nobody can look over your shoulder when you enter or write down personal information—at an ATM, filling out forms in public places, and so on
Minimize personal data shown on checks	Do not include a Social Security number or driver’s license number on your checks
Minimize time that mail is in your mailbox	Do not leave paid bills in your mailbox for postal pickup; collect mail from your mailbox as soon as possible after it is delivered
Do not use debit cards to pay for online purchases	Victims of credit card fraud are liable for no more than \$50 in losses; debit card users can have their entire checking account wiped out
Treat your credit card receipts safely	Always take your credit card receipts from the retailer and keep them for reconciliation purposes; dispose of them by shredding them
Use hard-to-guess passwords and PINs	Do not use names or words in passwords; include a mix of capital and small letters with at least one special character (\$, #, *)



Question & Answer Session





Computer Ethics & Society

Chapter # 5

Intellectual Property

ETHICS IN INFORMATION TECHNOLOGY BY GEORGE W. REYNOLDS

Prepared by: Shahid Hussain

WHAT IS INTELLECTUAL PROPERTY?

- Intellectual property is a term used to describe works of the mind—such as art, books, films, formulas, inventions, music, and processes—that are distinct, and owned or created by a single person or group. Intellectual property is protected through copyright, patent, and trade secret laws.



COPYRIGHTS

- A **copyright** is the exclusive right to distribute, display, perform, or reproduce an original work in copies or to prepare derivative works based on the work.
- Copyright protection is granted to the creators of “original works of authorship in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device.



Copyright infringement

- **Copyright infringement** is a violation of the rights secured by the owner of a copyright.
- Infringement occurs when someone copies a substantial and material part of another's copyrighted work without permission.



Eligible Works

- The types of work that can be copyrighted include architecture, art, audio-visual works, choreography, drama, graphics, literature, motion pictures, music, pantomimes, pictures, sculptures, sound recordings, and other intellectual works.



Fair Use Doctrine

- The fair use doctrine allows portions of copyrighted materials to be used without permission under certain circumstances.
- **Software Copyright Protection**
- To prove infringement, the copyright holder must show a striking resemblance between its software and the new software that could be explained only by copying.

PATENTS

- A **patent** is a grant of a property right issued by the United States Patent and Trademark Office (USPTO) to an inventor.
- A patent permits its owner to exclude the public from making, using, or selling a protected invention, and it allows for legal action against violators.

Patent infringement

- **Patent infringement**, or the violation of the rights secured by the owner of a patent, occurs when someone makes unauthorized use of another's patent.
- Unlike copyright infringement, there is no specified limit to the monetary penalty if patent infringement is found.

Continued....

- **Software Patents**
- A software patent claims as its invention some feature or process embodied in instructions executed by a computer.
- **Software Cross-Licensing Agreements**
- Many large software companies have cross-licensing agreements in which each party agrees not to sue the other over patent infringements.

TRADE SECRETS

- A **trade secret** is defined as business information that represents something of economic value, has required effort or cost to develop, has some degree of uniqueness or novelty, is generally unknown to the public, and is kept confidential.

Employees and Trade Secrets

- Employees are the greatest threat to the loss of company trade secrets—they might accidentally disclose trade secrets or steal them for monetary gain.
- Organizations must educate employees about the importance of maintaining the secrecy of corporate information.
- Trade secret information should be labeled clearly as confidential and should only be accessible by a limited number of people.
- Most organizations have strict policies regarding nondisclosure of corporate information.

KEY INTELLECTUAL PROPERTY ISSUES

- **Plagiarism**

- Plagiarism is the act of stealing someone's ideas or words and passing them off as one's own.

- **Reverse Engineering**

- Reverse engineering is the process of taking something apart in order to understand it, build a copy of it, or improve it.



Continued.....

- **Open Source Code**
- Open source code is any program whose source code is made available for use or modification, as users or other developers see fit.

- **Competitive Intelligence**
- Competitive intelligence is legally obtained information that is gathered to help a company gain an advantage over its rivals.



Continued.....

- **Cyber squatting**
- Cyber-squatters registered domain names for famous trademarks or company names to which they had no connection, with the hope that the trademark's owner would eventually buy the domain name for a large sum of money.
- A trademark is a logo, package design, phrase, sound, or word that enables a consumer to differentiate one company's products from another's.





Question & Answer Session





Computer Ethics & Society

Chapter # 6

Software Development

ETHICS IN INFORMATION TECHNOLOGY BY GEORGE W. REYNOLDS

Prepared by: Shahid Hussain

INTRODUCTION AND OVERVIEW

- High-quality software systems are easy to learn and use because they perform quickly and efficiently; they meet their users' needs; and they operate safely and reliably so that system downtime is kept to a minimum.
- Such software has long been required to support the fields of air traffic control, nuclear power, automobile safety, health care, military and defense, and space exploration.



Continued...

- Now that computers and software have become integral parts of almost every business, the demand for high-quality software is increasing.
- End users cannot afford system crashes, lost work, or lower productivity, nor can they tolerate security holes through which intruders can spread viruses, steal data, or shut down Web sites.
- Software manufacturers face economic, ethical, and organizational challenges associated with improving the quality of their software. This chapter covers many of these issues.

Continued....

- A **software defect** is any error that, if not removed, could cause a software system to fail to meet its users' needs.
- **Software quality** is the degree to which a software product meets the needs of its users.



Continued....

- **Quality management** focuses on defining, measuring, and refining the quality of the development process and the products developed during its various stages.
- These products—including statements of requirements, flowcharts, and user documentation—are known as **deliverables**.
- The objective of **quality management** is to help developers deliver high-quality systems that meet the needs of their users.



The Importance of Software Quality

- The accurate, thorough, and timely processing of business transactions is a key requirement for safety critical systems.
- A software defect can be devastating, resulting in lost customers and reduced revenue.



KEY ISSUES IN SOFTWARE DEVELOPMENT

- Although defects in any system can cause serious problems, the consequences of software defects in certain systems can be deadly.
- In these kinds of systems, the stakes involved in creating quality software are raised to the highest possible level.
- The ethical decisions involving a trade-off—if one must be considered—between quality and such factors as cost, ease of use, and time to market require extremely serious examination.

Development of Safety-Critical Systems

- A safety-critical system is one whose failure may cause injury or death.
- The safe operation of many safety-critical systems relies on the flawless performance of software;
- such systems control automobiles' antilock brakes, nuclear power plant reactors, airplane navigation, roller coasters, elevators, and numerous medical devices, to name just a few.

Continued....

- The process of building software for such systems require highly trained professionals, formal and rigorous methods, and state-of-the-art tools.
- However, even with these precautions, the software associated with safety-critical systems is still vulnerable to errors that can lead to injury or death.



Points to consider

- Consider the following points while developing safety critical systems:

- **International standards**

When developing safety-critical systems, a key assumption must be that safety will not automatically result from following an organization's standard development methodology.

- **Rigorous Software Development Process**

Safety-critical software must go through a much more rigorous and time-consuming development process than other kinds of software.



Continued....

- **Project safety engineer**

The key to ensuring that these additional tasks are completed is to appoint a project safety engineer, who has explicit responsibility for the system's safety.

- **Sufficient testing**

Another key issue is deciding when the QA staff has performed sufficient testing.

- **Formal risk analysis**

When designing, building, and operating a safety-critical system, a great deal of effort must be put into considering what can go wrong



Continued....

- **Redundancy**

Another key element of safety-critical systems is redundancy, the provision of multiple interchangeable components to perform a single function in order to cope with failures and errors.

- **Human Interface**

One of the most important and difficult areas of safety-critical system design is the human interface.



Quality Management Standards

- The International Organization for Standardization (ISO), founded in 1947, is a worldwide federation of national standards bodies from 161 countries.
- The ISO issued its 9000 series of business management standards in 1988.
- These standards require organizations to develop formal quality-management systems that focus on identifying and meeting the needs, desires, and expectations of their customers.



Continued....

- The ISO 9000 standard serves as a guide to quality products, services, and management. To obtain this coveted certificate, an organization must submit to an examination by an external assessor and fulfill the following requirements:
 - Have written procedures for all processes
 - Follow those procedures
 - Prove to an auditor that it has fulfilled the first two requirements; this proof can require observation of actual work practices and interviews with customers, suppliers, and employees.



Continued....

- The various ISO 9000 series of standards address the following software-related activities:
 - ISO 9001: Design, development, production, installation, servicing
 - ISO 9002: Production, installation, servicing
 - ISO 9003: Inspection and testing
 - ISO 9000-3: Development, supply, and maintenance of software
 - ISO 9004: Quality management and quality systems elements

Managers Checklist for improving software quality

TABLE 7-3 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?		



Question & Answer Session





Computer Ethics & Society

Chapter # 7

THE IMPACT OF INFORMATION TECHNOLOGY ON PRODUCTIVITY AND QUALITY OF LIFE

ETHICS IN INFORMATION TECHNOLOGY BY GEORGE W. REYNOLDS

Prepared by: Shahid Hussain

INTRODUCTION AND OVERVIEW

- The standard of living varies greatly among groups within a country as well as from nation to nation.
- The most widely used measurement of the material standard of living is gross domestic product (GDP) per capita.
- National GDP represents the total annual output of a nation's economy.
- Overall, industrialized nations tend to have a higher standard of living than developing countries.

IT Investment and Productivity

- **Productivity** is defined as the amount of output produced per unit of input, and it is measured in many different ways.
- **Innovation** is a key factor in productivity improvement, and IT has played an important role in enabling innovation.
- In the early days of IT in the 1960s, productivity improvements were easy to measure.
- Today, organizations are trying to further improve IT systems and business processes that have already gone through several rounds of improvement.



Tele-work

- **Tele-work** (also known as **telecommuting**) is a work arrangement in which an employee works away from the office—at home, at a client’s office, in a hotel—literally, anywhere.
- In Tele-work, an employee uses various forms of electronic communication, including e-mail, audio conferencing, video conferencing, and instant messaging.



Continued....

TABLE 8-3 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 tend to also 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 since 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.

Continued....

TABLE 8-4 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.



The Digital Divide

- Another indicator of the standard of living is the availability of technology.
- The **digital divide** is a term used to describe the gulf between those who do and those who don't have access to modern information and communications technology such as cell phones, personal computers, and the Internet.
- The digital divide exists not only between more and less developed countries but also within countries—among age groups, economic classes, and people who live in cities versus those in rural areas.



E-Rate Program

- The **Education Rate (E-Rate)** program was created through the Telecommunications Act of 1996.
- One of E-Rate's goals is to help schools and libraries obtain access to state-of-the-art services and technologies at discounted rates.
- The program's discounts range from 20 percent to 90 percent for eligible telecommunications services, depending on location (urban or rural) and economic need.

THE IMPACT OF IT ON HEALTHCARE COSTS

- The development and use of new medical technology, such as new diagnostic procedures and treatments (see Figure 8-2 in book), has increased spending and “accounts for one-half to two-thirds of the increase in healthcare spending in excess of general inflation.”
- Although many new diagnostic procedures and treatments are at least moderately more effective than their older counterparts, they are also more costly.
- To really gain control over soaring healthcare costs, patient awareness must be raised and technology costs must be managed more carefully.

Electronic Health Records

- An **electronic health record (EHR)** is a summary of health information generated by each patient encounter in any healthcare delivery setting.
- An EHR includes patient demographics, medical history, immunization records, laboratory data, problems, progress notes, medications, vital signs, and radiology reports.
- EHRs could incorporate data from any healthcare entity a patient uses and make the data easily accessible to other healthcare professionals.
- Healthcare professionals can use an EHR to generate a complete electronic record of a clinical patient encounter.

Use of Mobile and Wireless Technology in the Healthcare Industry

- The healthcare industry was actually a leader in adopting mobile and wireless technology.
- Common uses of wireless technology in the healthcare field include:
 - Providing a means to access and update EHRs at patients' bedsides to ensure accurate and current patient data
 - Enabling nurses to scan bar codes on patient wristbands and on medications to help them administer the right drug in the proper dosage at the correct time of day (an attached computer on a nearby cart is linked via a wireless network to a database containing physician medication orders)
 - Using wireless devices to communicate with healthcare employees wherever they may be

Telemedicine

- **Telemedicine** employs modern telecommunications and information technologies to provide medical care to people who live far away from healthcare providers.
- There are two basic forms of telemedicine: store-and-forward and live.
 - **Store-and-forward telemedicine** involves acquiring data, sound, images, and video from a patient and then transmitting everything to a medical specialist for later evaluation.
 - **Live telemedicine** requires the presence of patients and healthcare providers at the same time and often involves a video conference link between the two sites.



Medical Information Web Sites for Laypeople

- Healthy people as well as those who suffer from illness need reliable information on a wide range of medical topics to learn more about healthcare services and to take more responsibility for their health.
- Clearly, laypeople cannot become as informed as trained medical practitioners, but a tremendous amount of healthcare information is available via the Web.
- These sites have a critical responsibility to publish current, reliable, and objective information.
- Table 8-9 provides just a small sample of Web sites that offer information on a variety of medical-related topics.

Continued....

TABLE 8-9 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 what causes 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/	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.osteoporosis.nih.gov	The NIH 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



Question & Answer Session





Computer Ethics & Society

Chapter # 8

ETHICS OF IT ORGANIZATIONS

ETHICS IN INFORMATION TECHNOLOGY BY GEORGE W. REYNOLDS

Prepared by: Shahid Hussain

INTRODUCTION AND OVERVIEW

- This chapter will touch on the following ethical topics that are pertinent to organizations in the IT industry, as well as to organizations that make use of IT.
 - The use of non-traditional workers
 - Whistle-blowing
 - Green computing
 - Code to address ethical issues



KEY ETHICAL ISSUES FOR ORGANIZATIONS

- The use of nontraditional workers raises ethical issues for organizations.
- Whistle-blowing is an effort to attract public attention to a negligent, illegal, unethical, abusive, or dangerous act by a company or some other organization.
- Green computing is a term applied to a variety of efforts directed toward the efficient design, manufacture, operation, and disposal of IT-related products, including personal computers, laptops, servers, printers, and printer supplies.
- The electronics and information and communications technology (ICT) industry recognizes the need for a code to address ethical issues in the areas of worker safety and fairness, environmental responsibility, and business efficiency.



THE NEED FOR NON TRADITIONAL WORKERS

- **CONTINGENT WORKERS**

- The Bureau of Labor Statistics defines contingent work as a job situation in which an individual does not have an explicit or implicit contract for long-term employment.
- A firm is likely to use contingent IT workers if it experiences pronounced fluctuations in its technical staffing needs.
- Typically, these workers join a team of full-time employees and other contingent workers for the life of the project and then move on to their next assignment.



Advantages of Using Contingent Workers

- When a firm employs a contingent worker, it does not usually have to provide benefits such as insurance, paid time off, and contributions to a retirement plan.
- A company can easily adjust the number of contingent workers it uses to meet its business needs, and can release contingent workers when they are no longer needed.



Disadvantages of Using Contingent Workers

- One downside to using contingent workers is that they may not feel a strong connection to the company for which they are working.
- This can result in a low commitment to the company and its projects, along with a high turnover rate.



OUTSOURCING


- Outsourcing is another approach to meeting staffing needs.
- Outsourcing is a long-term business arrangement in which a company contracts for services with an outside organization that has expertise in providing a specific function.
- A company may contract with an organization to provide such services as operating a data center, supporting a telecommunications network, or staffing a computer help desk.



Offshore Outsourcing

- Offshore outsourcing is a form of outsourcing in which the services are provided by an organization whose employees are in a foreign country.
- Any work done at a relatively high cost in the United States may become a candidate for offshore outsourcing—not just IT work.
- However, IT professionals in particular can do much of their work anywhere—on company's premises or thousands of miles away in a foreign country.

WHISTLE-BLOWING

- **Whistle-blowing** is an effort to attract public attention to a negligent, illegal, unethical, abusive, or dangerous act by a company or some other organization.
 - In some cases, whistle-blowers are employees who act as informants on their company, revealing information to enrich themselves or to gain revenge for a perceived wrong.
 - In most cases, however, whistle-blowers act ethically in an attempt to correct what they think is a major wrongdoing, often at great personal risk.
 - A whistle-blower usually has personal knowledge of what is happening inside the offending organization because of his or her role as an employee of the organization.
 - Sometimes the whistle-blower is not an employee but a person with special knowledge gained from a position as an auditor or business partner.
- 

Continued....

- A potential whistle-blower must attempt to answer many ethical questions before making a decision on how to proceed:
 - Given the potentially high price, do I really want to proceed?
 - Have I exhausted all means of dealing with the problem? Is whistle-blowing all that is left?
 - Am I violating an obligation to be loyal to my employer and work for its best interests?
 - Will the public exposure of corruption and mismanagement in the organization really correct the underlying cause of these problems and protect others from harm?

GREEN COMPUTING

- Green computing is a term applied to a variety of efforts directed toward the efficient design, manufacture, operation, and disposal of IT-related products, including personal computers, laptops, servers, printers, and printer supplies.
- Many computer manufacturers today are talking about building a “green PC,” by which they usually mean one that uses less electricity to run than the standard computer; thus, its carbon footprint on the planet is smaller.
- The components of computers, in turn, are composed of many different materials, including some that are known to be potentially harmful to humans and the environment, including beryllium, cadmium, lead, mercury, brominated flame retardants, selenium, and polyvinyl chloride.
- Electronic manufacturing employees and suppliers at all steps along the supply chain and manufacturing process are at risk of unhealthy exposure to these raw materials.



ICT INDUSTRY CODE OF CONDUCT

- The Electronic Industry Citizenship Coalition (EICC) was established to promote a common code of conduct for the electronics and information and communications technology (ICT) industry.
- The following are the five areas of social responsibility and guiding principles covered by the code:
 - Labor:
 - Health and Safety:
 - Environment:
 - Management System:
 - Ethics:

Continued...

- **Labor:**

- “Participants are committed to uphold the human rights of workers, and to treat them with dignity and respect as understood by the international community.”

- **Health and Safety:**

- “Participants recognize that in addition to minimizing the incidence of work-related injury and illness, a safe and healthy work environment enhances the quality of products and services, consistency of production and worker retention and morale. Participants also recognize that on-going worker input and education is essential to identifying and solving health and safety issues in the workplace.”

- **Environment:**

- “Participants recognize that environmental responsibility is integral to producing world class products. In manufacturing operations, adverse effects on the community, environment, and natural resources are to be minimized while safeguarding the health and safety of the public.”

- **Management System:**

- “Participants shall adopt or establish a management system whose scope is related to the content of this Code. The management system shall be designed to ensure
- (a) Compliance with applicable laws, regulations and customer requirements related to the participant’s operations and products;
- (b) Conformance with this Code; and
- (c) Identification and mitigation of operational risks related to this Code. It should also facilitate continual improvement.”

- **Ethics:**

- “To meet social responsibilities and to achieve success in the marketplace, participants and their agents are to uphold the highest standards of ethics including: business integrity; no improper advantage; disclosure of information; intellectual property; fair business, advertising, and competition; and protection of identity.”



Question & Answer Session

