Ch1: Overview of Ethics

1.WHAT IS ETHICS?

Q.1 What is Ethics? Why it is important to act according to code of ethics? W/13 & S/15 CSE , S/14 IT S/15 CT

‣Each society forms a set of rules that set up 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 that are so widely shared that they become the basis for an established consensus.
‣However, individual views of what is moral may vary by age, cultural group, ethnic background, religion, life experiences, education, and gender.
‣There is widespread agreement on the immorality of murder, theft, and arson, but other behaviors that are accepted in one culture might be unacceptable in another.
‣Even within the same society, people can have strong disagreements over important moral issues.

1.1 . Definition of Ethics:

Q. Define Ethics? Describe the importance of Integrity. S/14 CT

•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. However, although nearly everyone would agree that lying and cheating are unethical, opinions about what constitutes ethical behavior often vary dramatically.
• For example, attitudes toward software piracy that is, the practice of illegally making copies of software or enabling others to access software to which they are not entitled range from strong opposition to acceptance of the practice as a standard approach to conducting business.

1.2. The Importance of Integrity:

•Your moral principles are statements of what you believe to be rules of right conduct. As a child, you may have been taught not to lie, cheat, or steal. As an adult facing more complex decisions, you often reflect on your principles when you consider what to do in different situations: Is it okay to lie to protect someone's feelings?
•A person who acts with integrity acts in accordance with a personal code of principles. One approach to acting with integrity one of the foundations of ethical behavior—is to extend to all people the same respect and consideration that you expect to receive from others. Unfortunately, consistency can be difficult to achieve, particularly when you are in a situation that conflicts with your moral standards.
•For example, you might believe it is important to do as your employer requests while also believing that you should be fairly rewarded for your work. Thus, if your employer insists that you do not report the overtime hours that you have worked due to budget constraints, a moral conflict arises. You can do as your employer requests or you can insist on being fairly rewarded, but you cannot do both. In this situation, you may be forced to compromise one of your principles and act with an apparent lack of integrity
•Another form of inconsistency emerges if you apply moral standards differently according to the situation or people involved. To be consistent and act with integrity, you must apply the same moral standards in all situations.

1.3. The Difference between Morals, Ethics, and Laws:

Q. Describe the difference between Morals, Ethics & laws W/13, & W/14 CT

•Morals are one's personal beliefs about right and wrong, while the term ethics describes standards or codes of behavior expected of an individual by a group (nation, organization, profession) to which an individual belongs.
•For example, the ethics of the law profession demand that defense attorneys defend an accused client to the best of their ability, even if they know that the client is guilty of the most heinous and morally objectionable crime one could imagine
•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 with what an individual believes to be the right thing to do. Laws can proclaim an act as legal, although many people may consider the act immoral—for example, abortion

1.4. ETHICS IN THE BUSINESS WORLD:

Q. What are Ethics in Business world S/15 CT, S/15 CSE
Q. What is org. doing to improve their business ethics? W/14 CSE & W/14 IT

•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.
•In the past decade, we have seen the failure of major corporations such as Enron and WorldCom due to accounting scandals**.**
•We have watched the collapse of financial institutions due to unwise and unethical decision making over the approval of mortgages and lines of credit to unqualified individuals and organizations
•unethical behavior has led to serious negative consequences that have had a major global impact.
•Several trends have increased the likelihood of unethical behavior. First, for many organizations, greater globalization has created a much more complex work environment that spans diverse cultures and societies, making it much more difficult to apply principles and codes of ethics consistently. For example, numerous U.S. companies have garnered negative publicity for moving operations to third-world countries, where employees work in conditions that would not be acceptable in most developed parts of the world.
•Second, in today's recessionary economic climate, organizations are extremely challenged to maintain revenue and profits. Some organizations are sorely tempted to resort to unethical behavior to maintain profits. For example, the Peanut Corporation of America allegedly shipped tainted products from its plant in Georgia, which led to a salmonella outbreak in 2008 that killed at least eight people and sickened over 550 people in 43 states
•Employees, shareholders, and regulatory agencies are increasingly sensitive to violations of accounting standards, failures to disclose substantial changes in business conditions, nonconformance with required health and safety practices, and production of unsafe or substandard products. Such heightened vigilance raises the risk of financial loss for businesses that do not foster ethical practices or that run afoul of required standards. There is also a risk of criminal and civil lawsuits resulting in fines and/or incarceration for individuals.

1.5 . Why Fostering (Development) Good Business Ethics Is Important:

Q. What is Ethics? Why are organization interested in fostering Good Business Ethics S/14 & W/14 CSE & W/14 S/14 IT

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

1.5.1 Gaining the Good Will of the Community:

•Although organizations exist primarily to earn profits or provide services to customers, they also have some fundamental responsibilities to society**.**
•"Technology companies are waking up to the fact that they have to attract and maintain loyalty with their customers," says Carol Cone, head of Boston marketing consulting firm Cone, Inc., which helps develop corporate giving programs.
•Many organizations initiate or support socially responsible activities, which include making contributions to charitable organizations and nonprofit institutions, providing benefits for employees in excess of any legal requirements, and devoting organizational resources to initiatives that are more socially desirable than profitable.

1.5.2. Creating an Organization That Operates Consistently

•Organizations develop and stand by values to create an organizational culture and to define a consistent approach for dealing with the needs of their stakeholders—shareholders, employees, customers, suppliers, and the community. Such consistency means that employees know what is expected of them and can employ the organization's values to help them in their decision making**.**

•Consistency also means that shareholders, customers, suppliers, and the community know what they can expect of the organization—that it will behave in the future much as it has in the past.

•It is especially important for multinational or global organizations to present a consistent face to their shareholders, customers, and suppliers no matter where those stakeholders live or operate their business.

Although each company's value system is different, many 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 organization
- Value diversity
- Make decisions based on facts and principles

1.5.3. Fostering Good Business Practices:

•In many cases, good ethics can mean good business and improved profits. Companies that produce safe and effective products avoid costly recalls and lawsuits. Companies that provide excellent service retain their customers instead of losing them to competitors. Companies that develop and maintain strong employee relations suffer lower turnover rates and enjoy better employee morale. Suppliers and other business partners often place a priority on working with companies that operate in a fair and ethical manner.

•bad ethics can have a negative impact on employees, many of whom can develop negative attitudes if they perceive a difference between their own values and those stated or implied by an organization's actions.

‣ In such an environment, employees may suppress their tendency to act in a manner that seems ethical to them and instead act in a manner that will protect them against anticipated punishment.

‣When such a discrepancy between employee and organizational ethics occurs, it destroys employee commitment to organizational goals and objectives, creates low morale, fosters poor performance, erodes employee involvement in organizational improvement initiatives, and builds indifference to the organization's needs.

1.5.4 Protecting the Organization and Its Employees from Legal Action:

A coalition of several legal organizations, including the Association of Corporate Counsel, the U.S. Chamber of Commerce, the National Association of Manufacturers, the National Association of Criminal Defense Lawyers, and the New York State Association of Criminal Defense Lawyers, argues that organizations should be able to escape criminal liability if they have acted as responsible corporate citizens, making strong efforts to prevent and detect misconduct in the workplace."

One way to do this is to establish effective ethics and compliance programs.

Indeed, in 1991, the Department of Justice established sentencing guidelines that suggest more lenient treatment for convicted executives if their companies have ethics programs. Fines for criminal violations can be lowered by up to 80 percent if the organization has implemented an ethics management program and cooperates with authorities.

1.5.5 Avoiding Unfavorable Publicity:

The public reputation of a company strongly influence the value of its stock, how consumers regard its products and services, the degree of oversight it receives from government agencies, and the amount of support and cooperation it receives from its business partners.

Thus, many organizations are motivated to build a strong ethics program to avoid negative publicity. If an organization is perceived as operating ethically, customers, business partners, shareholders, consumer advocates, financial institutions, and regulatory bodies will usually regard it more favorably.

1.6 . Improving Corporate Ethics:

Q. How to improve corporate ethics? W/13 & S/14 CT

Research by the Ethics Resource Center found that only one in four organizations has a well-implemented ethics and compliance program. The Ethics Resource Center has defined the following characteristics of a successful ethics program:

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

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.

1.6.1 Appointing a Corporate Ethics Officer:

•A corporate ethics officer(also called a corporate compliance officer) provides an organization with vision and leadership in the area of business conduct.

• Organizations send a clear message to employees about the importance of ethics and compliance in their decision about who will be in charge of the effort and to whom that individual will report.

• Ideally, the corporate ethics officer should be a well-respected, senior-level manager who reports directly to the CEO. Ethics officers come from diverse backgrounds, such as legal staff, human resources, finance, auditing, security, or line operations.

1.6.2 Ethical Standards Set by Board of Directors:

•The board of directors is responsible for the careful and responsible management of an organization. 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.

•The board fulfills some of its responsibilities directly and assigns others to various committees.

•The board is not normally responsible for day-to-day management and operations; these responsibilities are delegated to the organization's management team. However, the board is responsible for supervising the management team.

•Board members are expected to conduct themselves according to the highest standards for personal and professional integrity, while setting the standard for company-wide ethical conduct and ensuring compliance with laws and regulations. •Employees will"get the message" if board members set an example of high-level ethical behavior. If they don't set a good example, employees will get that message as well.

1.6.3 Establishing a Corporate Code of Ethics:

•A code of ethics is a statement that highlights an organization's key ethical issues and identifies the overarching values and principles that are important to the organization and its decision making.

• The code frequently includes a set of formal, written statements about the purpose of the organization, its values, and the principles that should guide its employees' actions. An organization's code of ethics applies to its directors, officers, and employees.

•The code of ethics focuses employees on areas of ethical risk relating to their role in the organization, offers guidance to help them recognize and deal with ethical issues, and provides mechanisms for reporting unethical conduct and fostering a culture of honesty and accountability within the organization.

• The code of ethics helps ensure that employees abide by the law, follow necessary regulations, and behave in an ethical manner.

1.6 .4 Conducting Social Audits:

•An increasing number of organizations conduct social audits of their policies and practices.

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

•This information is shared with employees, shareholders, investors, market analysts, customers, suppliers, government agencies, and the communities in which the organization operates.

1.6.5 Requiring Employees to Take Ethics Training:

‣The ancient Greek philosophers believed that personal convictions about right and wrong behavior could be improved through education. Today, most psychologists agree with them.

‣Lawrence Kohlberg, the late Harvard psychologist, found that many factors stimulate a person's moral development, but one of the most crucial is education.

‣Other researchers have repeatedly supported the idea that people can continue their moral development through further education, such as working case studies and examining contemporary issues.

‣Thus, an organization's code of ethics must be promoted and continually communicated within the organization, from top to bottom.

‣Organizations can do this by showing employees examples of how to apply the code of ethics in real life. One approach is through a comprehensive ethics education program that encourages employees to act responsibly and ethically.

‣Such programs are often presented in small workshop formats in which employees apply the organization's code of ethics to hypothetical but realistic case studies.

‣Employees may also be given examples of recent company decisions based on principles from the code of ethics.

‣ It is critical that such training increase the percentage of employees who report incidents of misconduct; thus, employees must be shown effective ways of reporting such incidents.

‣ In addition, they must be reassured that such feedback will be acted on and that they will not be subjected to retaliation.

1.6.6 Including Ethical Criteria in Employee Appraisals:

‣Managers can ensure that employees are meeting performance expectations if they monitor employee behavior and provide feedback; however, a recent survey of HR professionals revealed that only 43 percent of organizations include ethical conduct as part of an employee' s performance appraisal.

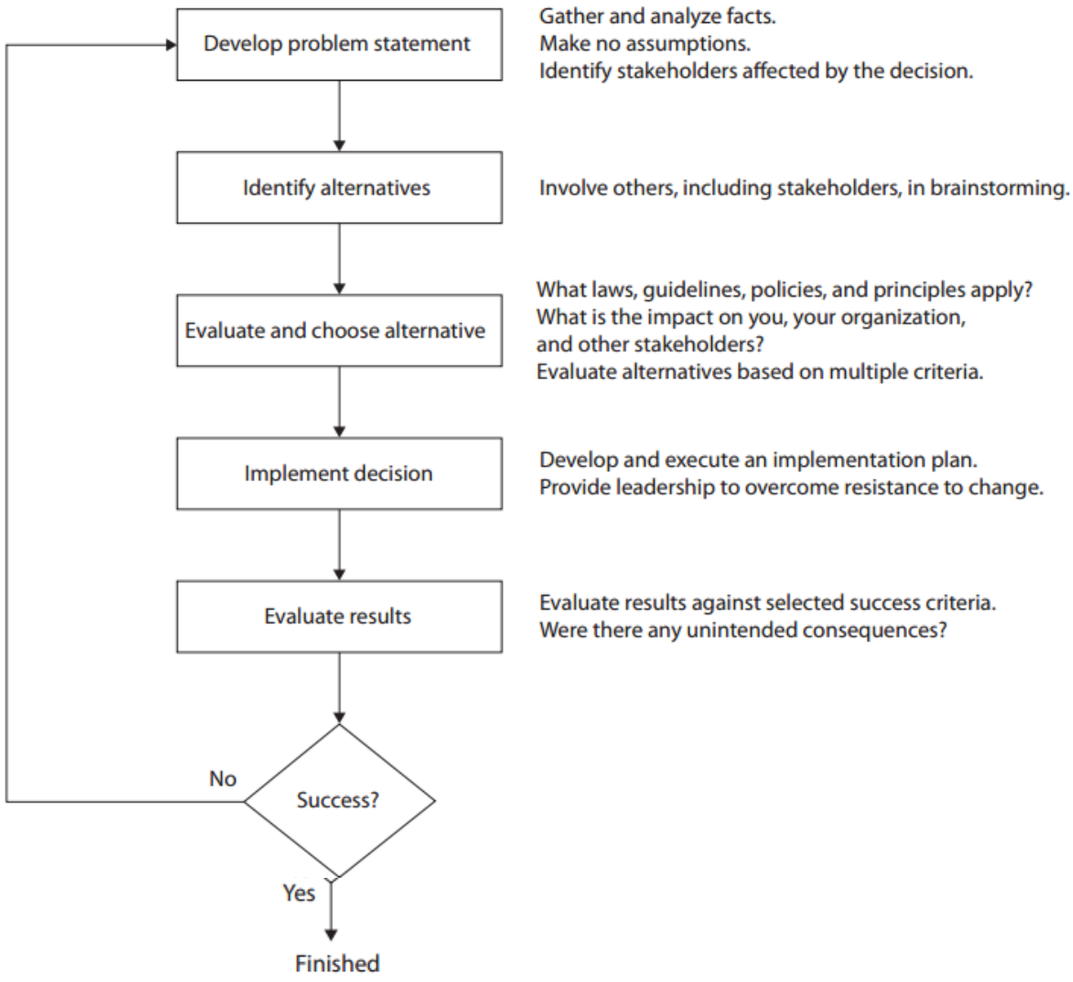
‣Those that do so base a portion of their employees' performance evaluations on treating others fairly and with respect; operating effectively in a multicultural environment; accepting personal accountability for meeting business needs; continually developing others and themselves; and operating openly and honestly with suppliers, customers, and other employees.

‣These factors are considered along with the more traditional criteria used in performance appraisals, such as an employee's overall contribution to moving the business ahead, successful completion of projects and tasks, and maintenance of good customer relations.

1.7. Ethical Considerations in Decision Making:

Q. Describe 4 common approaches to Ethical decision making. W/13 & S/15 CSE & S/14 IT S/15 CT

We are all faced with difficult decisions in our work and in our personal life. Most of us have developed a decision-making process that we execute automatically, without thinking about the steps we go through. For many of us, the process generally follows the steps outlined in Figure



1.7.1 Develop a Problem Statement

‣A problem statement is a clear, brief description of the issue that needs to be addressed. A good problem statement answers the following questions: What do people observe that causes them 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? Development of a problem statement is the most critical step in the decision-making process.

‣Without a clear statement of the problem or the decision to be made, it is useless to proceed. Obviously, if the problem is stated incorrectly, the decision will not solve the problem.

‣One must gather and analyze facts to develop a good problem statement. Seek information and opinions from a variety of people to expand your frame of reference. During this process, you must be extremely careful not to make assumptions about the situation. Simple situations can sometimes turn into complex controversies because no one takes the time to gather the facts.

‣For example, you might see your boss receive what appears to be an employment application from a job applicant and then throw the application into the trash after the applicant leaves.

‣This would violate your organization's policy to treat each applicant with respect and to maintain a record of all applications for one year.

‣You could report your boss for failure to follow the policy, or you could take a moment to speak directly to your boss. You might be pleasantly surprised to find out that the situation was not as it appeared.

‣Perhaps the "applicant" was actually a salesperson promoting a product for which your company had no use, and the "application" was marketing literature.

‣Part of developing a good problem statement involves identifying the stakeholders and their positions on the issue. Stakeholders often include others beyond those directly involved in an issue. Identifying the stakeholders helps you understand the impact of your decision and could help you make a better decision.

‣ unfortunately, it may also cause you to lose sleep from wondering how you might affect the lives of others. By involving stakeholders in the decision, you gain their support for the recommended course of action. What is at stake for each stakeholder? What does each stakeholder value, and what outcome does each stakeholder want? Do some stakeholders have a greater stake because they have special needs or because the organization has special obligations to them? To what degree should they be involved in the decision?

1.7.2 Identify Alternatives:

‣During this stage of decision making, it is ideal to enlist the help of others, including stakeholders, to identify several alternative solutions to the problem. Brainstorming with just one other person will reduce your chances of identifying a broad range of alternatives and determining the best solution.

‣On the other hand, there are times when it is inappropriate to involve others in solving a problem that you are not at liberty to discuss.

‣ In providing participants information about the problem to be solved, offer just the facts, without your opinion, so you don't influence others to accept your solution.

‣During any brainstorming process, try not to be critical of ideas, as any negative criticism will tend to "shut down" the group, and the flow of ideas will dry up. Simply write down the ideas as they are suggested.

1.7.3 Evaluate and Choose an Alternative:

‣Once a set of alternatives has been identified, the group attempts to evaluate them based on numerous criteria, such as effectiveness at addressing the issue, the extent of risk associated with each alternative, cost, and time to implement.

‣An alternative that sounds attractive but that is not feasible will not help solve the problem.

‣As part of the evaluation process, weigh various laws, guidelines, and principles that may apply. You certainly do not want to violate a law that can lead to a fine or imprisonment for yourself or others.

‣Are there any corporate policies or guidelines that apply? Does the organizational code of ethics offer guidance? Do any of your own personal principles apply? Also consider the likely consequences of each alternative from several perspectives

‣What is the impact on you, your organization, other stakeholders (including your suppliers and customers), and the environment? The alternative selected should be ethically and legally defensible; be consistent with the organization's policies and code of ethics; take into account the impact on others; and, of course, provide a good solution to the problem.

1.7.4 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.

‣It does not define a formula for ethical decision making, but suggests that when faced with a complex ethical dilemma, people do either what they are most comfortable doing or what they think a person they admire would do.

‣The assumption is that people are guided by their virtues to reach the "right" decision.

‣A supporter of virtue ethics believes that a disposition to do the right thing is more effective than following a set of principles and rules, and that people should perform moral acts out of habit, not introspection.

‣Virtue ethics can be applied to the business world by equating the virtues of a good business person with those of a good person.

‣However, business people face situations that are peculiar to business, so they may need to tailor their ethics accordingly.

‣For example, honesty and sincerity when dealing with others are generally considered virtuous; however, a corporate purchasing manager who is negotiating a multimillion dollar deal might need to be vague in discussions with potential suppliers.

1.7.5 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.

‣The goal is to find the single greatest good by balancing the interests of all affected parties.

‣Utilitarianism fits easily with the concept of value in economics and the use of cost-benefit analysis in business.

‣Business managers, legislators, and scientists weigh the benefits and harm of policies when deciding whether to invest resources in building a new plant in a foreign country, to enact a new law, or to approve a new prescription drug.

1.7.6 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. However, decisions made with this approach can be influenced by personal bias toward a particular group, and the decision makers may not even realize their bias.

‣If the intended goal of an action or a policy is to provide benefits to a target group, other affected groups may consider the decision unfair.

1.7.7 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.

‣Decisions and policies that use this approach attempt to implement social systems,\ institutions, and environments that everyone depends on and that benefit all people. ‣Examples include an effective education system, a safe and efficient transportation system, and accessible and affordable health care.

1.7.8 Implement Decision

Once the alternative is selected, it should be implemented in an efficient, effective, and timely manner. This is much easier said than done, since people tend to resist change. In fact, the bigger the change, the greater is the resistance to it. Communication is the key to helping people accept a change

1.7.9 Evaluate the Results

After the solution to the problem has been implemented, monitor the results to see if the desired effect was achieved, and observe its impact on the organization and the various stakeholders.

1.8. ETHICS IN INFORMATION TECHNOLOGY:

Q. What trends have increased risk of using information Technology in unethical manner? W/13 IT S/14 CSE

‣The growth of the Internet, the ability to capture and store vast amounts of personal data, and greater reliance on information systems in all aspects of life have increased the risk that information technology will be used unethically.

‣ In the midst of the many IT breakthroughs in recent years, the importance of ethics and human values has been underemphasized— with a range of consequences.

‣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, 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.

1.9 Conflict of Interest:

Q. Define the Term Conflict of Interest and provide an IT related example of this W/13 S/14 CT

‣A **conflict of interest** (**COI**) is a situation in which a person or organization is involved in multiple interests (financial, emotional, or otherwise), one of which could possibly corrupt the motivation of the individual or organization.

‣The presence of a conflict of interest is independent of the occurrence of impropriety. Therefore, a conflict of interest can be discovered and voluntarily defused before any corruption occurs.

‣A widely used definition is: "A conflict of interest is a set of circumstances that creates a risk that professional judgment or actions regarding a primary interest will be unduly influenced by a secondary interest."

‣ Primary interest refers to the principal goals of the profession or activity, such as the protection of clients, the health of patients, the integrity of research, and the duties of public office.

‣Secondary interest includes not only financial gain but also such motives as the desire for professional advancement and the wish to do favors for family and friends, but conflict of interest rules usually focus on financial relationships because they are relatively more objective, fungible, and quantifiable.

‣The secondary interests are not treated as wrong in them, but become objectionable when they are believed to have greater weight than the primary interests. The conflict in a conflict of interest exists whether or not a particular individual is actually influenced by the secondary interest.

‣It exists if the circumstances are reasonably believed (on the basis of past experience and objective evidence) to create a risk that decisions may be unduly influenced by secondary interests.

Types of Possible Conflicts
Independence in Choosing Licensees

There are a variety of possible street from which UC can choose for licensing a discovery or invention, such as a new company established for the specific purpose of bringing the invention to market. Often the choice is directed to a company which can best market the invention/discovery and has the capability to commercialize the product with wide dissemination. The importance of transfer of a technology is recognized as essential to the success of the venture. In making these decisions, the issue of personal gain of the researcher must be addressed. This requires the complete disclosure on the part of the researcher about involvement with companies under consideration, as the royalties awarded through the license will be adjusted to take into consideration any company holdings of the researcher.

Business Involvement in Research Field

A member of the faculty or staff is considered to have a potential conflict of interest if, in dealings with the University, the best interests of the University could be compromised in the personal interest of the faculty or staff member or in the interests of an external company or agency in which the individual has a significant interest. "Significant interest" implies that, as a result of affiliation with an outside organization (formal or informal), the individual can influence that organization's decisions to the detriment of UC.

Examples of significant interest that could lead to this situation include but are not limited to:

1. Purchasing/Selling Procedures

The University's approach to avoiding conflicts of interest in purchasing and selling is to deal at arm's length with suppliers and customers by appointing agents authorized to make decisions on purchasing and selling who are separate from units and individuals standing to benefit from the purchase/sale.

2. Purchasing

All faculty and staff members who have decision-making authority or who are in a position to influence a decision about a purchase or contract must disclose in writing any personal material interest in a

prospective vendor to the Director of Purchasing and withdraw from the decision-making process, if that is deemed appropriate.

3. Selling

A conflict is considered to exist whenever a personal consideration, benefit or material interest could potentially interfere with optimizing the dollar return to UC on its goods or services sold. For this reason, the establishment of prices at fair market value and the dissemination of information about the availability for sale of goods and services are critical.

All faculty and staff members who have decision-making authority or who are in a position to influence a decision about a sale must disclose any personal material interest in the transaction to the vice president to whom their department reports, copying administrative heads and/or deans, and withdraw from the sale process if deemed appropriate.

1.1 Social audit:

Q. What is Social audit? What area is it likely to encompass & in whom is it communicate? W/14 CT

•In asocial audit, an organization reviews how well it is meeting its ethical and social responsibility goals, and communicates its new goals for the upcoming year.
•This information is shared with employees, shareholders, investors, market analysts, customers, suppliers, government agencies, and the communities in which the organization operates.
•For example, each year Intel prepares its Corporate Responsibility Report, which summarizes the firm's progress toward meeting its ethical and social responsibility goals.

•A social audit looks at factors such as a company's record of charitable giving, volunteer activity, energy use, transparency, work environment and worker pay and benefits to evaluate what kind of social and environmental impact a company is having in the locations where it operates.

•Social audits are optional--companies can choose whether to perform them and whether to release the results publicly or only use them internally.

•In the era of corporate social responsibility, where corporations are often expected not just to deliver value to consumers and shareholders but also to meet environmental and social standards deemed desirable by some vocal members of the general public, social audits can help companies create, improve and maintain a positive public relations image.

• Good public relations is key because the way a company is perceived will usually have an impact on its bottom line.

1.11 compliance

Q. What is meant by compliance? How does it help to promote the right behaviors & discourage undesirable ones?

•In general, **compliance** means conforming to a rule, such as a specification, policy, standard or law.

•**Regulatory compliance** describes the goal that organisations aspire to achieve in their efforts to ensure that they are aware of and take steps to comply with relevant laws and regulations.

•Due to the increasing number of regulations and need for operational transparency, organizations are increasingly adopting the use of consolidated and harmonized sets of compliance controls.

•This approach is used to ensure that all necessary governance requirements can be met without the unnecessary duplication of effort and activity from resources.

Standards and regulations

•The International Organization for Standardisation (ISO) produces international standards such as ISO17799.

•The International Electrotechnical Commission (IEC) produces international standards in the electro technology area.

•The ISO 19600:2014 standard provides a reminder of how compliance and risk should operate together, as "colleagues" sharing a common framework with some nuances to account for their differences.
•Some local or international specialized organizations such as the American Society of Mechanical Engineers (ASME) also develop standards and regulation codes.

•They thereby provide a wide range of rules and directives to ensure compliance of the products to safety, security or design standards.

•There are a number of other regulations which apply in different fields, such as PCI-DSS, GLBA, FISMA, Joint Commission and HIPAA. In some cases other compliance frameworks (such as COBIT) or standards (NIST) inform on how to comply with the regulations.

CHAPTER2

ETHICS FOR IT WORKERS AND IT USERS

2. What is IT PROFESSIONALS?

•A profession is a calling that requires specialized knowledge and often long and intensive academic preparation.

•Over the years, the United States government adopted labor laws and regulations that required a more precise definition of what is meant by a professional Employee.

The U.S. Code of Federal Regulations defines a 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.

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.

•In other words, professionals such as doctors, lawyers, and accountants require advanced training and experience; they must exercise discretion and judgment in the course of their work; and their work cannot be standardized.

‣Many people would also expect professionals to contribute to society, to participate in a lifelong training program (both formal and informal), to keep abreast of developments in their field, and to assist other professionals in their development.

‣ In addition, many professional roles carry special rights and responsibilities. Doctors, for example, prescribe drugs, perform surgery, and request confidential patient information while maintaining doctor–patient confidentiality.

Are IT Workers Professionals?

Q. What key characteristics distinguish a professional from other kinds of workers and is an IT worker considered a professional? S/14 CSE

,•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).

,• One could argue, however, that not every IT role requires “knowledge of an advanced type in a field of science or learning customarily acquired by a prolonged course of specialized intellectual instruction and study,”to quote again from the U.S. Code of Federal Regulations.

,•From alegal perspective, IT workers are not recognized as professionals because they are not licensed by the state or federal government.

,• for example, in malpractice lawsuits, as many courts have ruled that IT workers are not liable for malpractice because they do not meet the legal definition of a professional.

2.1 The Changing Professional Services Industry:

Q. Explain the different nature of professional services industry? S/15 CT S/14 W/14IT W/13 CSE

Although not legally classified as professionals, IT workers are considered part of the professional services industry, which is experiencing immense changes that impact how members of this industry must think and behave to be successful. Ross Dawson, author and CEO of the consulting firm Advanced Human Technology, identifies seven forces that are changing the nature of professional services: client sophistication, governance, connectivity, transparency, modularization, globalization, and commoditization.

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.

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.

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.

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.

2.2 Professional Relationships That Must Be Managed

Q. Discuss Professional relationship IT workers must manage. S/14 S/15 CT W/14 CSE

IT workers typically become involved in many different relationships, including those with employers, clients, suppliers, other professionals, IT users, and the society at large. In each relationship, an ethical IT worker acts honestly and appropriately.

2.2.1 Relationships between IT Workers and Employers:

•IT workers and employers have a critical, multifaceted relationship that requires ongoing effort by both parties to keep it strong.

• An IT worker and an employer typically agree on fundamental aspects of this relationship before the worker accepts an employment offer.

•These issues can include job title, general performance expectations, specific work responsibilities, drug-testing requirements, dress code, location of employment, salary, work hours, and company benefits.

• Many other issues are addressed in the company's policy and procedures manual or in the company's code of conduct, if one exists.

• These issues include protection of company secrets; vacation policy; time off for a funeral or an illness in the family; tuition reimbursement; and use of company resources, including computers and networks.

•Other aspects of the relationship develop over time as the need arises (for example, whether the employee can leave early one day if the time is made up another day).

•Some aspects are addressed by law—for example, an employee cannot be required to do anything illegal, such as falsify the results of a quality assurance test.

•Some aspects are specific to the role of the IT worker and are established based on the nature of the work or project—for example, the programming language to be used, the type and amount of documentation to be produced, and the extent of testing to be conducted.

2.2.2 Relationships between IT Workers and Clients:

‣An IT worker often provides services to clients who either work outside the worker's own organization or are"internal."

‣In relationships between IT workers and clients, each party agrees to provide something of value to the other. Generally speaking, the IT worker provides hardware, software, or services at a certain cost and within a given time frame.

‣For example, an IT worker might agree to implement a new accounts payable software package that meets the client's requirements. The client provides compensation, access to key contacts, and perhaps a work space.

‣This 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. Although there is often a vast disparity in technical expertise between IT workers and their clients, the two parties must work together to be successful.

‣Typically, the client makes decisions about a project on the basis of information, alternatives, and recommendations provided by the IT worker. The client trusts the IT worker to use his or her expertise and to act in the client's best interests.

‣The IT worker must trust that the client will provide relevant information, listen to and understand what the IT worker says, ask questions to understand the impact of key decisions, and use the information to make wise choices among various alternatives. Thus, the responsibility for decision making is shared between client and IT worker.

‣One potential ethical problem that can interfere with the relationship between IT workers and their clients involves IT consultants or auditors who recommend their own products and services or those of an affiliated vendor to remedy a problem they have detected.

‣ for example, an IT consulting firm might be hired to assess a firm's IT strategic plan. After a few weeks of analysis, the consulting firm might provide a poor rating for the existing strategy and insist that its proprietary products and services are required to develop a new strategic plan. Such findings raise questions about the vendor's objectivity and whether its recommendations can be trusted.

‣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.

‣The project manager may want to keep resources flowing into the project and hope that problems can be corrected before anyone notices.

‣ The project manager may also be reluctant to share status information because of contractual penalties for failure to meet the schedule or to develop certain system functions.

‣In this situation, the client may not be informed about the problem until it has become a crisis. After the truth comes out, finger-pointing and heated discussions about cost overruns, missed schedules, and technical incompetence can lead to charges of fraud, misrepresentation, and breach of contract.

‣Fraud is the crime of obtaining goods, services, or property through deception or trickery. Fraudulent misrepresentation occurs when a person consciously decides to induce another person to rely and act on the misrepresentation.

‣To prove fraud in a court of law, 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.

2.2.3 Relationships Between IT Workers and Suppliers:

‣IT workers deal with many different hardware, software, and service providers. Most IT workers understand that building a good working relationship with suppliers encourages the flow of useful communication as well as the sharing of ideas. Such information can lead to innovative and cost-effective ways of using the supplier's products and services that the IT worker may never have considered.

‣IT workers should develop good relationships with suppliers by dealing fairly with them and not making unreasonable demands.

‣Threatening to replace a supplier, who can't deliver needed equipment tomorrow, when the normal industry lead time is one week, is aggressive behavior that does not help a working relationship.

‣Suppliers strive to maintain positive relationships with their customers in order to make and increase sales.

‣ To achieve this goal, they may sometimes engage in unethical actions—for example, offering an IT worker a gift that is actually intended as a bribe. Clearly, IT workers should not accept a bribe from a vendor, and they must be careful in considering what constitutes a bribe.

‣For example, accepting invitations to expensive dinners or payment of entry fees for a golf tournament may seem innocent to the recipient, but it may be perceived as bribery by an auditor.

‣Bribery involves providing money, property, or favors to someone in business or government to obtain a business advantage.

‣An obvious example is a software supplier sales representative who offers money to another company's employee to get its business.

‣This type of bribe is often referred to as a kickback or a payoff. The person who offers a bribe commits a crime when the offer is made, and the recipient is guilty of bribery upon accepting the offer.

‣Various states have enacted bribery laws, which have sometimes been used to invalidate contracts involving bribes but have seldom been used to make criminal convictions.

Distinguishing between bribes and gifts

Q. Difference between bribe and gift W/13 IT

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

2.2.4 Relationships Between IT Workers and Other Professionals

‣Professionals feel a degree of loyalty to the other members of their profession. As a result, they are quick to help each other obtain new positions but slow to criticize each other in public.

‣Professionals also have an interest in their profession as a whole, because how it is perceived affects how individual members are seen and treated.

‣(For example, politicians are not generally thought to be very trustworthy, but teachers are.) Hence, professionals owe each other an adherence to the professions code of conduct.

‣Experienced professionals can also serve as mentors and help develop new members of the profession.

‣A number of ethical problems can arise among members of the IT profession. One of the most common is résumé inflation, which involves lying on a résumé and claiming competence in an IT skill that is in high demand.

‣Even though an IT worker might benefit in the short term from exaggerating his or her qualifications, such an action can hurt the profession and the individual in the long run.

‣Customers—and society in general—might become much more skeptical of IT workers as a result.

‣Some studies have shown that around 30 percent of all job applicants exaggerate their accomplishments, while roughly 10 percent“ seriously misrepresent”their backgrounds.

‣Another ethical issue is the 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.

2.2.5 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—subject, of course, to budget and time constraints.

‣ IT workers also have a key responsibility to establish an environment that supports ethical behavior by users. Such an environment discourages software piracy, minimizes the inappropriate use of corporate computing resources, and avoids the inappropriate sharing of information.

2.2.6 Relationships Between IT Workers and Society

‣Regulatory laws establish safety standards for products and services to protect the public. However, these laws are less than perfect, and they fail to safeguard against all negative side effects of a product or process.

‣Often, professionals can clearly see what effect their work will have and can take action to eliminate potential public risks.

‣Thus, society expects members of a profession to provide significant benefits and to not cause harm through their actions. One approach to meeting this expectation is to establish and maintain professional standards that protect the public.

‣the actions of an IT worker can affect society. For example, a systems analyst may design a computer-based control system to monitor a chemical manufacturing process.

‣A failure or an error in the system may put workers or residents near the plant at risk.

‣As a result, IT workers have a relationship with society members who may be affected by their actions.

‣However, there is currently no single, formal organization of IT workers that takes responsibility for establishing and maintaining standards that protect the public.

2.3 Professional Codes of Ethics

Q. What is professional code of Ethics? W/14 CT

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

‣ Practitioners in many professions subscribe to a code of ethics that governs their behavior.

‣For example, doctors adhere to varying versions of the 2000-year-old Hippocratic oath, which medical schools offer as an affirmation to their graduating classes.

‣Most codes of ethics created by professional organizations have two main parts:

‣the first outlines what the organization aspires to become, and the second typically lists rules and principles by which members of the organization are expected to abide.

‣Many codes also include a commitment to continuing education for those who practice the profession.

‣Laws do not provide a complete guide to ethical behavior. Just because an activity is not defined as illegal does not mean it is ethical.

‣You also cannot expect a professional code of ethics to provide an answer to every ethical dilemma—no code can be the definitive collection of behavioral standards. However, following

a professional code of ethics can produce many benefits for the individual, the 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.

‣The code also defines behaviors that are acceptable and unacceptable to guide professionals in their interactions with others.

‣Strong codes of ethics have procedures for censuring professionals for serious violations, with penalties that can include the loss of the right to practice. Such codes are the exception, however, and few exist in the IT arena.

• Trust and respect from the general public—Public trust is built on the expectation that a professional will behave ethically.

‣People must often depend on the integrity and good judgment of a professional to tell the truth, abstain from giving self-serving advice, and offer warnings about the potential negative side effects of their actions.

‣Thus, adherence to a code of ethics enhances trust and respect for professionals and their profession.

• Evaluation benchmark—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.

2.4 Certification:

‣Certification indicates that a professional possesses a particular set of skills, knowledge, or abilities, in the opinion of the certifying organization.

‣ Unlike licensing, which applies only to people and is required by law, certification can also apply to products (e.g., 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) and is generally voluntary.

‣ IT-related certifications may or may not include a requirement to adhere to a code of ethics, whereas such a requirement is standard with licensing.

‣Numerous companies and professional organizations offer certifications, and opinions are divided on their value. Many employers view them as a benchmark that indicates mastery of a defined set of basic knowledge.

‣On the other hand, because certification is no substitute for experience and doesn’t guarantee that a person will perform well on the job, some hiring managers are rather cynical about the value of certifications.

‣Most IT employees are motivated to learn new skills, and certification provides a structured way of doing so.

‣ For such people, completing a certification provides clear recognition and correlates with a plan to help them continue to grow and advance in their careers. Others view certification as just another means for product vendors to generate additional revenue with little merit attached.

2.4.1 Vendor Certifications

‣Many IT vendors—such as Cisco, IBM, Microsoft, Sun, SAP, and Oracle—offer certification programs for their products.

‣Workers who successfully complete a program can represent Them selves as certified users of a manufacturer's product.

‣Depending on the job market and the demand for skilled workers, some certifications might substantially improve an IT worker's salary and career prospects.

‣Certifications that are tied to a vendor's product are relevant for job roles with very specific requirements or certain aspects of broader roles.

‣Sometimes, however, vendor certifications are too focused on technical details of the vendor's technology and do not address more general concepts To become certified, one must pass a written exam.

‣ Because of legal concerns about whether other types of exams can be graded objectively, most exams are presented in a multiple-choice format.

2.4.2 Industry Association Certifications

‣There are many industry certifications in a variety of IT-related subject areas . Their value varies greatly depending on where people are in their career path, what other certifications they possess, and the nature of the IT job market.

‣ For example, according to a 2007 study by Foote Partners LLC, formally certified security professionals are generally paid at least 10 percent more than noncertified individuals.

‣The requirements for certification generally require that the individual has the prerequisite education and experience, sits for and passes an exam, and commits to and abides by a code of ethics established by the organization providing the certification.

‣In order to remain certified, the individual must typically pay an annual certification fee, earn continuing education credits, and—in some cases—pass a periodic renewal test.

2.5 Government Licensing:

‣In the United States, a government license is government-issued permission to engage in an activity or to operate a business.

‣ It is generally administered at the state level and often requires that the recipient pass a test of some kind. Some professionals must be licensed, including certified public accountants (CPAs), lawyers, doctors, various types of medical and day-care providers, and some engineers.

2.5.1 The Case for Licensing IT Workers

‣The days of simple, stand-alone information systems are over.

‣Modern systems are highly complex, interconnected, and critically dependent on one another. Highly integrated enterprise resource planning (ERP) systems help multibillion-dollar companies control all of their business functions, including forecasting, production planning, purchasing, inventory control, manufacturing, and distribution.

‣ Complex computers and information systems manage and control the nuclear reactors of power plants that generate electricity. Medical information systems monitor the vital statistics of hospital patients on critical life support.

‣Every year, local, state, and federal government information systems are entrusted with generating and distributing millions of checks worth billions of dollars to the public.

▪As a result of the increasing importance of IT in our everyday lives, the development of reliable, effective information systems has become an area of mounting public concern.

▪This concern has led to a debate about whether the licensing of IT workers would improve information systems.

▪Proponents argue that licensing would strongly encourage IT workers to follow the highest standards of the profession and practice a code of ethics.

▪Licensing would also allow for violators to be punished. Without licensing, there are no requirements for heightened care and no concept of professional malpractice.

2.6 IT Professional Malpractice:

Q. Short note on IT professional Malpractice W/14 S/15 IT

‣Negligence has been defined as not doing something that a reasonable person would do, or doing something that a reasonable person would not do.

‣Duty of carerefers to the obligation to protect people against any unreasonable harm or risk.

‣For example, people have a duty to keep their pets from attacking others and to operate their cars safely.

‣Similarly, businesses must keep dangerous pollutants out of the air and water, make safe products, and maintain safe operating conditions for employee.

▪Professionals who breach the duty of care are liable for injuries that their negligence causes. This liability is commonly referred to as professional malpractice.

▪For example, a CPA who fails to use reasonable care, knowledge, skill, and judgment when auditing a client's books is liable for accounting malpractice. Professionals who breach this duty are liable to their patients or clients, and possibly to some third parties.

▪Courts have consistently rejected attempts to sue individual parties for computer-related malpractice. Professional negligence can only occur when people fail to perform within the standards of their profession, and software engineering is not a uniformly licensed profession in the United States.

▪ Because there are no uniform standards against which to compare a software engineer's professional behavior, he or she cannot be subject to malpractice lawsuits.

2.7 IT USERS:

Common Ethical Issues for IT Users:

Q. What is the common ethical issue for IT users? W/13 W/14 CT, W/13 IT

2.7.1 Software Piracy

‣software piracy in a corporate setting can sometimes be directly traceable to IT professionals—they might allow it to happen, or they might actively engage in it. ‣Corporate IT usage policies

and management should encourage users to report instances of piracy and to challenge its practice.

‣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.

‣ When confronted, the IT user's argument might be:"I bought a home computer partly so I could take work home and be more productive; therefore, I need the same software on my home computer as I have at work."However, if no one has paid for an additional license to use the software on the home computer, this is still piracy

2.7.2 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.

‣These activities eat away at worker productivity and waste time. Furthermore, activities such as viewing sexually explicit material, sharing lewd jokes, and sending hate e-mail could lead to lawsuits and allegations that a company allowed a work environment conducive to racial or sexual harassment.

‣According to a survey by Harris Interactive, 16 percent of men and 8 percent of women with Internet access at work acknowledged that they had seen pornography in the workplace.

‣Companies often fire frequent pornography offenders and take disciplinary action against less egregious offenders. After a month long investigation of computer usage habits of Washington, D.C., municipal workers, nine employees were fired and an unspecified number of employees were sanctioned for visiting pornographic Web sites while at work.

2.7.3 Inappropriate Sharing of Information

‣Every organization stores vast amounts of information that can be classified as either private or confidential.

‣Private data describes individual employees—for example, their salary information, attendance data, health records, and performance ratings. Private data also includes information about customers—credit card information, telephone number, home address, and so on. Confidential information describes a company and its operations, including sales and promotion plans, staffing projections, manufacturing processes, product formulas, tactical and strategic plans, and research and development.

‣ An IT user who shares this information with an unauthorized party, even inadvertently, has violated someone's privacy or created the potential that company information could fall into the hands of competitors.

‣ For example, if an IT employee saw a coworker's payroll records and then discussed them with a friend, it would be a clear violation of the coworker's privacy

2.8 Multilayer Process

Q. What is the key element of a multilayer process for managing security vulnerabilities based on the concept of reasonable assurance? S/14 IT W/14 CSE

- Key elements of a multilayer process for managing security vulnerabilities include:
  - Assessment
  - User education
  - Response plan

▪**A vulnerability assessment** is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system.

▪Examples of systems for which vulnerability assessments are performed include, but are not limited to, information technology systems, energy supply systems, water supply systems, transportation systems, and communication systems.

▪ Such assessments may be conducted on behalf of a range of different organizations, from small businesses up to large regional infrastructures. Vulnerability from the perspective of disaster management means assessing the threats from potential hazards to the population and to infrastructure.

▪ It may be conducted in the political, social, economic or environmental fields.

Vulnerability assessment has many things in common with risk assessment. Assessments are typically performed according to the following steps:

1. Cataloging assets and capabilities (resources) in a system.
2. Assigning quantifiable value (or at least rank order) and importance to those resources
3. Identifying the vulnerabilities or potential threats to each resource
4. Mitigating or eliminating the most serious vulnerabilities for the most valuable resources

An incident response plan (IRP) is a set of written instructions for adequately detecting, responding to and limiting the effects of an information security incident, an event that may or may not be an attack or threat to computer system or corporate data security.

2.9 Safety critical system

Q. Discuss issue of development of safety critical system S/14 CT

safety-critical system is a system whose failure or malfunction may result in one (or more) of the following outcomes:

- death or serious injury to people
- loss or severe damage to equipment/property
- environmental harm

▪Risks of this sort are usually managed with the methods and tools of safety engineering. A life-critical system is designed to lose less than one life per billion (10^9) hours of operation.

▪ Typical design methods include probabilistic risk assessment, a method that combines failure mode and effects analysis (FMEA) with fault tree analysis. Safety-critical systems are increasingly computer-based.

Reliability rule

Several reliability regimes for life-critical systems exist:

- **Fail-operational systems** continue to operate when their control systems fail. Examples of these include elevators, the gas thermostats in most home furnaces, and passively safe nuclear reactors. Fail-operational mode is sometimes unsafe. Nuclear weapons launch-on-loss-of-communications was rejected as a control system for the U.S. nuclear forces because it is fail-operational: a loss of communications would cause launch, so this mode of operation was considered too risky. This is contrasted with the Fail-deadly behavior of the Perimeter system built during the Soviet era.[2]
- **Fail-safe systems** become safe when they cannot operate. Many medical systems fall into this category. For example, an infusion pump can fail, and as long as it alerts the nurse and ceases pumping, it will not threaten the loss of life because its safety interval is long enough to permit a human response. In a similar vein, an industrial or domestic burner controller can fail, but must fail in a safe mode (i.e. turn combustion off when they detect faults). Famously, nuclear weapon systems that launch-on-command are fail-safe, because if the communications systems fail, launch cannot be commanded. Railway signaling is designed to be fail-safe.
- **Fail-secure** systems maintain maximum security when they can not operate. For example, while fail-safe electronic doors unlock during power failures, fail-secure ones will lock, keeping an area secure.
- **Fail-Passive systems** continue to operate in the event of a system failure. An example includes an aircraft autopilot. In the event of a failure, the aircraft would remain in a controllable state and allow the pilot to take over and complete the journey and perform a safe landing.
- **Fault-tolerant systems** avoid service failure when faults are introduced to the system. An example may include control systems for ordinary nuclear reactors. The normal method to tolerate faults is to have several computers continually test the parts of a system, and switch on hot spares for failing subsystems. As long as faulty subsystems are replaced or repaired at normal maintenance intervals, these systems are considered safe. Interestingly, the computers, power supplies and control terminals used by human beings must all be duplicated in these systems in some fashion.

2.10 falsehood or exaggeration

Q. Enlist most frequent areas of resume falsehood or exaggeration W/13 S/15 IT

▪According to Accu-Screen Inc., a Tampa, Fla., company that specializes in employment background screening of job applicants, the most common resume lies are exaggerations and inflated numbers including dates of employment, salary and fictitious job titles.

▪Bogus degrees and imaginary certifications are less commons, but frequent enough, the company reports.

▪The company is expert at how and how often job seekers lie, having tracked the findings of extensive employment background checks since its 1994 inception.

▪Accu-Screen's reference checks reveal 8 percent of accomplishments listed in resume job descriptions to be, at best, exaggerations, and 18 percent of resumes include fake companies or lie about companies no longer in business.

Here are the top seven places where honesty slips off the resume page, gleaned from the company's 15 years of recorded fibs, exaggerations and flat-out lies:

1. Dates of employment

It's understandable to be a little fuzzy on dates, but when years of tenure creep in to a job description, an applicant is likely hiding employment gaps.

Where they'll find the truth: A thorough reference check.

2. Job title

Resumes magically give promotions more often than do employers, according to Accu-Screen's data. A fudged job title often goes hand-in-hand with inflated salary on job applications.

Where they'll find the truth: A thorough reference check.

3. Criminal records

People understandably fear that their job applications will be rejected if they have a criminal history and will lie about this history regardless of how serious or trivial their crime. A much more serious prospect is presented by those who intend to repeat their criminal activity, whether it's embezzling or criminal negligence.

Where they'll find the truth: A criminal background check.

4. Inflated salary

Confidentiality issues often prevent employers from divulging salary information. Sneaky job applicants can and do use this to inflate their salaries and thereby improve their bargaining position.

Where they'll find the truth: A thorough reference check.

5. Education (e.g., bogus degrees)

Accu-Screen estimates that 16 percent of academic degrees and institutions listed on resumes are falsified. Job seekers also falsify 15 percent of technical skills and certifications.

That includes the job seeker graduating him- or herself, claiming a degree when none was earned. Some dishonest job seekers go so far as to steal another person's identity by borrowing their educational credentials.

Where they'll find the truth: Background screening includes verifying educational claims with universities and other training facilities.

6. Professional license (MD, RN, CPA, et al.)

Beyond just "graduating" themselves, some dishonest job applicants are hitching unearned titles to their names. This is an especially egregious lie, given that employers are legally liable and can suffer serious financial penalties for falsely passing off employees as being credentialed.

Where they'll find the truth: Background screening includes verifying licenses with accrediting agencies.

7. "Ghost" company (self-owned business)

Just because you spent a few weeks putting a new roof on your mother's house doesn't mean you owned and ran your own carpentry and construction business for a number of years.

According to Accu-Screen, applicants are currently falsifying 18 percent of past employers by making up fictitious companies or by falsifying or exaggerating information about a company that's gone out of business. Job seekers may also use this tactic to cover up employment gaps.

▪**Exaggeration** can be a rhetorical device or figure of speech. It may be used to evoke strong feelings or to create a strong impression.

▪Amplifying achievements, obstacles and problems to seek attention is an everyday occurrence Inflating the difficulty of achieving a goal after attaining it, can be used to bolster self-esteem.

▪In the arts, exaggerations are used to create emphasis or effect. As a literary device, exaggerations is often used in poetry, and is frequently encountered in casual speech Many times the usages of hyperbole describes something as better or worse than it really is.

▪ An example of hyperbole is: "The bag weighed a ton." Hyperbole makes the point that the bag was very heavy, though it probably does not weigh a ton.

▪Exaggerating is also a type of deception, as well as a means of malingering - magnifying small injuries or discomforts as an excuse to avoid responsibilities.

▪Alarmism is excessive or exaggerated alarm about a real or imagined threats

CHAPTER3

COMPUTER AND INTERNET CRIME

3. IT SECURITY INCIDENTS: A MAJOR CONCERN:

Q. Explain various factor causing increase in the number of computer related security incident in recent years? S/14 W/14 IT
Q. What action must be taken in response to a security incident? W/13 S/14 W/14 CSE W/13 CT S/14 CT S/15 CSE

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. Business managers, IT professionals, and IT users all face a number of ethical decisions regarding IT security:

• If their firm is a victim of a computer crime, should they pursue prosecution of the criminals at all costs, maintain a low profile to avoid the negative publicity, inform their affected customers, or take some other action?

• How much effort and money should be spent to safeguard against computer crime? (In other words, how safe is safe enough?)

• If their firm produces software with defects that allow hackers to attack customer data and computers, what actions should they take?

• What should be done if recommended computer security safeguards make life more difficult for customers and employees, resulting in lost sales and increased costs?

Why Computer Incidents Are So Prevalent?

Increasing Complexity Increases Vulnerability

The computing environment has become enormously complex. Networks, computers, operating systems, applications, Web sites, switches, routers, and gateways are interconnected and driven by hundreds of millions of lines of code. This environment continues to increase in complexity every day. The number of possible entry points to a network expands continually as more devices are added, increasing the possibility of security breaches.

Higher Computer User Expectations

Today, time means money, and the faster computer users can solve a problem, the sooner they can be productive. As a result, computer help desks are under intense pressure to respond very quickly to users' questions. Under duress, help desk personnel sometimes forget to verify users' identities or to check whether they are authorized to perform a requested action. In addition, even though they have been warned against doing so, some computer users share their login ID and password with other coworkers who have forgotten their own passwords. This can enable workers to gain access to information systems and data for which they are not authorized.

Expanding and Changing Systems Introduce New Risks

Business has moved from an era of stand-alone computers, in which critical data was stored on an isolated mainframe computer in a locked room, to an era in which personal computers connect to networks with millions of other computers, all capable of sharing information. Businesses have moved quickly into e-commerce, mobile computing, collaborative work groups, global business, and inter organizational information systems. Information technology has become

ubiquitous and is a necessary tool for organizations to achieve their goals. However, it is increasingly difficult to keep up with the pace of technological change, successfully perform an ongoing assessment of new security risks, and implement approaches for dealing with them

Increased Reliance on Commercial Software with Known Vulnerabilities:

▪In computing, an exploit is an attack on an information system that takes advantage of a particular system vulnerability. Often this attack is due to poor system design or implementation.

▪Once the vulnerability is discovered, software developers quickly create and issue a "fix,"or patch, to eliminate the problem. Users of the system or application are responsible for obtaining and installing the patch, which they can usually download from the Web.

▪(These fixes are in addition to other maintenance and project work that software developers perform.) Any delay in installing a patch exposes the user to a security breach.

▪Estimates of the rate at which software vulnerabilities are discovered by organizations around the world vary widely; the daily rate has been estimated to be as low as seven vulnerabilities and as high as 382.

▪All these bugs and potential vulnerabilities create a serious work overload for developers, who are responsible for security fixes.

▪Clearly, it can be difficult to keep up with all the required patches. Azero-day attacktakes place before the security community or software developer knows about the vulnerability or has been able to repair it.

▪ Although the potential for damage from zero-day exploits is great, few such attacks have been documented as of this writing.

3.1 Types of Exploits:

Q. Elaborate most common types of Security attack W/13, S/14 IT W/13, S/14, W/14 CSE W/14, S/15 CT
Q. Define the terms virus, worms, Trojan horse root kits W/14 IT

3.1 .1 Viruses

▪Computer virus has become an umbrella term for many types of malicious code. Technically, avirusis a piece of programming code, usually disguised as something else, that causes a computer to behave in an unexpected and usually undesirable manner.

▪Often a virus is attached to a file, so that when the infected file is opened, the virus executes. Other viruses sit in a computer's memory and infect files as the computer opens, modifies, or creates them.

▪ Most viruses deliver a"payload,"or malicious software that causes the computer to perform in an unexpected way.

▪For example, the virus may be programmed to display a certain message on the computer's display screen, delete or modify a certain document, or reformat the hard drive.

▪A true virus does not spread itself from computer to computer. A virus is spread to other machines when a computer user opens an infected e-mail attachment, downloads an infected program, or visits infected Web sites. In other words, it takes action by the "infected"computer user to spread a virus.

▪Macro viruses have become a common and easily created form of virus.

▪Attackers use an application macro language (such as Visual Basic or VBScript) to create programs that infect documents and templates.

▪After an infected document is opened, the virus is executed and infects the user's application templates. Macros can insert unwanted words, numbers, or phrases into documents or alter command functions.

▪ After a macro virus infects a user's application, it can embed itself in all future documents created with the application

3.1.2 Worms:

▪A **computer worm** is a standalone malware computer program that replicates itself in order to spread to other computers.

▪Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it.

▪ Unlike a computer virus, it does not need to attach itself to an existing program.

▪ Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

3.1.3 Trojan Horses:

▪A Trojan horse is a program in which malicious code is hidden inside a seemingly harmless program.

▪The program's harmful payload can enable the hacker to destroy hard drives, corrupt files, control the computer remotely, launch attacks against other computers, steal passwords or Social Security numbers, and spy on users by recording keystrokes and transmitting them to a server operated by a third party.

▪A Trojan horse can be delivered as an e-mail attachment, downloaded from a Web site, or contracted via a removable media device such as a CD/DVD or USB memory stick.

▪ Once an unsuspecting user executes the program that hosts the Trojan horse, the malicious payload is automatically launched as well—with no telltale signs. Common host programs include screen savers, greeting card systems, and games.

▪Work is the suite of applications created by Apple that includes word processing, desktop publishing, presentation preparation software, and a spreadsheet application.

▪Some pirated copies of this software contain a Trojan horse, iServices.a, which launches when the user begins installation of the pirated software.

▪ When installed, the Trojan horse"phones home"to the hacker's server to confirm the Mac is infected and awaits further instructions.

3.1.4 Botnets

▪A 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.

▪The collective processing capacity of some botnets exceeds that of the world's most powerful supercomputers.

▪Cutwail, a large botnet, controlled approximately one million active bots at one time.

▪It is estimated that about one in four personal computers in the United States is part of a botnet

3.1.5 Distributed Denial-of-Service (DDoS) Attacks:

▪A distributed denial-of-service attack (DDoS)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.

▪A distributed denial-of-service attack does not involve infiltration of the targeted system. Instead, it keeps the target so busy responding to a stream of automated requests that legitimate users cannot get in—the Internet equivalent of dialing a telephone number repeatedly so that all other callers hear a busy signal.

▪The targeted machine"holds the line open"while waiting for a reply that never comes, and eventually the requests exhaust all resources of the target.

▪The software to initiate a denial-of-service attack is simple to use and readily available at 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.

▪Based on a command by the attacker or at a preset time, these 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 zombies involved in a denial-of-service attack are often seriously compromised and are left with more enduring problems than their target.

▪As a result, zombie machines need to be inspected to ensure that the attacker software is completely removed from the system.

▪In addition, system software must often be reinstalled from a reliable backup to reestablish the system's integrity, and an upgrade or patch must be implemented to eliminate the vulnerability that allowed the attacker to enter the system.

3.1.6 Rootkits:

▪A 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.

▪ Once installed, the attacker can gain full control of the system and even obscure the presence of the rootkit from legitimate system administrators.

▪Attackers can use the rootkit to execute files, access logs, monitor user activity, and change the computer's configuration. Rootkits are one part of a blended threat, consisting of the dropper, loader, and rootkit.

▪The dropper code 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.

▪The dropper launches the loader program and then deletes itself.

▪The loader loads the rootkit into memory; at that point the computer has been compromised. Rootkits are designed so cleverly that it is difficult to even discover if they are installed on a computer.

▪The fundamental problem with trying to detect a rootkit is that the operating system currently running cannot be trusted to provide valid test results. Here are some symptoms of rootkit infections:

• The computer locks up or fails to respond to input from the keyboard ormouse.

• The screen saver changes without any action on the part of the user.

• The taskbar disappears.

• Network activities function extremely slowly.

▪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.

3.1.7 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, sometimes for questionable products such as pornography, phony get-rich-quick schemes, and worthless stock. Spam is also an extremely inexpensive method of marketing used by many legitimate organizations.

▪For example, a company might send e-mail to a broad cross section of potential customers to announce the release of a new product in an attempt to increase initial sales. Spam may also be used to deliver harmful worms or other malware.

▪The cost of creating an e-mail campaign for a product or service is several hundred to a few thousand dollars, compared to tens of thousands of dollars for direct-mail campaigns.

▪In addition, e-mail campaigns take only a couple of weeks to develop, compared with three months or more for direct-mail campaigns, and the turnaround time for feedback averages 48 hours for e-mail as opposed to weeks for direct mail.

▪However, the benefits of spam to companies can be largely offset by the public's generally negative reaction to receiving unsolicited ads.

▪Spam forces unwanted and often objectionable material into e-mail boxes, detracts from the ability of recipients to communicate effectively due to full mailboxes and relevant e-mails being hidden among many unsolicited messages, and costs Internet users and service providers millions of dollars annually.

▪ It takes users time to scan and delete spam e-mail, a cost that can add up if they pay for Internet connection charges on an hourly basis.

▪It also costs money for ISPs and online services to transmit spam, which is reflected in the rates charged to all subscribers.

3.1.8 Phishing:

▪Phishing is the act of using e-mail fraudulently to try to get the recipient to reveal personal data.

▪In a phishing scam, con artists send legitimate looking e-mails 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 e-mail attachment.

▪These e-mails, such as , lead consumers to counterfeit Web sites designed to trick them into divulging personal data.

▪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. eBay, PayPal, and Citibank are among the Web sites that phishers spoof most frequently.

▪Spear-phishing is a variation of phishing in which the phisher sends fraudulent e-mails to a certain organization's employees.

▪ The phony e-mails are designed to look like they came from high-level executives within the organization.

▪Employees are again directed to a fake Web site and then asked to enter personal information, such as name, Social Security number, and network passwords.

FIGURE Example of phishing

3.2 Comparison chart

Q. Difference between virus and worms W/13 CT

Computer Virus	Computer Worm

	Computer Virus	Computer Worm
How does it infect a computer system?	It inserts itself into a file or executable program.	It exploits a weakness in an application or operating system by replicating itself.
How can it spread?	It has to rely on users transferring infected files/programs to other computer systems.	It can use a network to replicate itself to other computer systems without user intervention.
Does it infect files?	Yes, it deletes or modifies files. Sometimes a virus also changes the location of files.	Usually not. Worms usually only monopolize the CPU and memory.
whose speed is more?	virus is slower than worm.	worm is faster than virus. E.g.The code red worm affected 3 lack PCs in just 14 Hrs.
Definition	The virus is the program code that attaches itself to application program and when application program run it runs along with it.	The worm is code that replicate itself in order to consume resources to bring it down.

3.3 Types of Perpetrators:

Q. Who are the primary perpetrators of computer crime and what are their objectives? S/14 , W/14 IT, S/14, W/14 S/15 CSE S/15 CT

3.3.1 Hackers and Crackers:

▪Hackers test the limitations of information systems out of intellectual curiosity—to see whether they can gain access and how far they can go.

▪ They have at least a basic understanding of information systems and security features, and much of their motivation comes from a desire to learn even more. The term hacker has evolved over the years, leading to its negative connotation today rather than the positive one it used to have.

▪ While there is a vocal minority who believe that hackers perform a service by identifying security weaknesses, most people now believe that a hacker no longer has the right to explore public or private networks.

▪Some hackers are smart and talented, but many are technically inept and are referred to as lamers or script kiddies by more skilled hackers.

▪ Surprisingly, hackers have a wealth of available resources to hone their skills—online chat groups, Web sites, downloadable hacker tools, and even hacker conventions (such as DEFCON, an annual gathering in Las Vegas).

▪**Cracking** is a form of hacking that is 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, and writing scripts and automated programs that let other people do the same things.

▪For example, crackers defaced a CERN (the European Organization for Nuclear Research) Web page, disparaging CERN'sIT security staff as a"bunch of school kids"and saying they had no plan to disrupt CERN's operations but simply wanted to highlight the lab's security problems.

3.3.2 Malicious Insiders:

Q. What may be the protection mechanisms against malicious insiders? W/13 W/14CT

▪A major security concern for companies is the malicious insider—an ever present and extremely dangerous adversary, as shown in the opening vignette.

▪ Companies are exposed to a wide range of fraud risks, including diversion of company funds, theft of assets, fraud connected with bidding processes, invoice and payment fraud, computer fraud, and credit card fraud.

▪Not surprisingly, fraud that occurs within an organization is usually due to weaknesses in its internal control procedures.

▪As a result, many frauds are discovered by chance and by outsiders—via tips, through resolving payment issues with contractors or suppliers, or during a change of management—rather than through control procedures.

▪Often, frauds involve some form of collusion, or cooperation, between an employee and an outsider.

▪insiders are not necessarily employees; they can also be consultants and contractors.

▪However,"the 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."

▪The risk tolerance of these employees depends on whether they are motivated by financial gain, revenge on their employers, or publicity.

▪Malicious insiders are extremely difficult to detect or stop because they are often authorized to access the very systems they abuse.

▪Although insiders are less likely to attack systems than outside hackers or crackers are, the company's systems are far more vulnerable to them.

▪Most computer security measures are designed to stop external attackers but are nearly powerless against insiders. Insiders have knowledge of individual systems, which often includes the procedures to gain access to login IDs and passwords.

▪Insiders know how the systems work and where the weak points are. Their knowledge of organizational structure and security procedures helps them avoid investigation of their actions.

▪There are several steps organizations can take to reduce the potential for attacks from insiders, including the following:

• Perform a thorough background check as well as psychological and drug testing

of candidates for sensitive positions.

• Establish an expectation of regular and ongoing psychological and drug testing as a normal routine for people in sensitive positions.

• Carefully limit the number of people who can perform sensitive operations, and grant only the minimum rights and privileges necessary to perform essential duties

• Define job roles and procedures so that it is not possible for the same person to both initiate and approve an action.

• Periodically rotate employees in sensitive positions so that any unusual procedures can be detected by the replacement.

• Immediately revoke all rights and privileges required to perform old job responsibilities when someone in a sensitive position moves to a new position.

• Implement an ongoing audit process to review key actions and procedures

3.3.3 Industrial Spies:

▪Industrial spies use illegal means to obtain trade secrets from competitors of their sponsor.

▪Trade secrets are protected by the Economic Espionage Act of 1996, which makes it a federal crime to use a trade secret for one's own benefit or another's benefit.

▪Trade secrets are most often stolen by insiders, such as disgruntled employees and ex-employees. Competitive intelligence uses legal techniques to gather information that is available to the public.

▪ Participants gather and analyze information from financial reports, trade journals, public filings, and printed interviews with company officials. Industrial espionage involves using illegal means to obtain information that is not available to the public.

▪ Participants might place a 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.

▪An unethical firm may spend a few thousand dollars to hire an industrial spy to steal trade secrets that can be worth a thousand times that amount.

The industrial spy avoids taking risks that would expose his employer, as the employer's reputation (an intangible but valuable item) would be considerably damaged if the espionage were discovered.

3.3.4 Cybercriminals:

Q. Difference between cybercriminals and cyberteeriost W/13 IT

▪Information technology provides a new and highly profitable venue for cybercriminals, who are attracted to the use of information technology for its ease in reaching millions of potential victims.

▪ Cybercriminals are motivated by the potential for monetary gain and hack into corporate computers to steal, often by transferring money from one account to another to another—leaving a hopelessly complicated trail for law enforcement officers to follow.

▪Cybercriminals also engage in all forms of computer fraud—stealing and reselling credit card numbers, personal identities, and cell phone IDs. Because the potential for monetary

Hacktivists and Cyber terrorists

Hacktivism, a combination of the words hacking and activism, is hacking to achieve a political or social goal. A cyber terrorist launches computer-based attacks against other computers or networks in an attempt to intimidate or coerce a government in order to advance certain political or social objectives. Cyber terrorists are more extreme in their goals than hacktivists although there is no clear demarcation line. Because of the Internet, cyber attacks can easily originate from foreign countries, making detection and retaliation much more difficult.

3.4 IMPLEMENTING TRUSTWORTHY COMPUTING:

▪Trustworthy computing is a method of computing that delivers secure, private, and reliable computing experiences based on sound business practices; this is what organizations worldwide are demanding today.

• Everyone who provides computing services (software and hardware manufacturers, consultants, programmers) knows that this is a priority for their customers The security of any system or network is a combination of technology, policy, and people and requires a wide range of activities to be effective.

▪"Society ultimately expects computer systems to be trustworthy—that is, that they do what is required and expected of them despite environmental disruption, human user and operator errors, and attacks by hostile parties, and that they not do other things."

▪A strong security program begins by assessing threats to the organization's computers and network, identifying actions that address the most serious vulnerabilities, and educating end users about the risks involved and the actions they must take to prevent a security incident.

▪The IT security group must lead the effort to prevent security breaches by implementing security policies and procedures, as well as effectively employing available hardware and software tools.

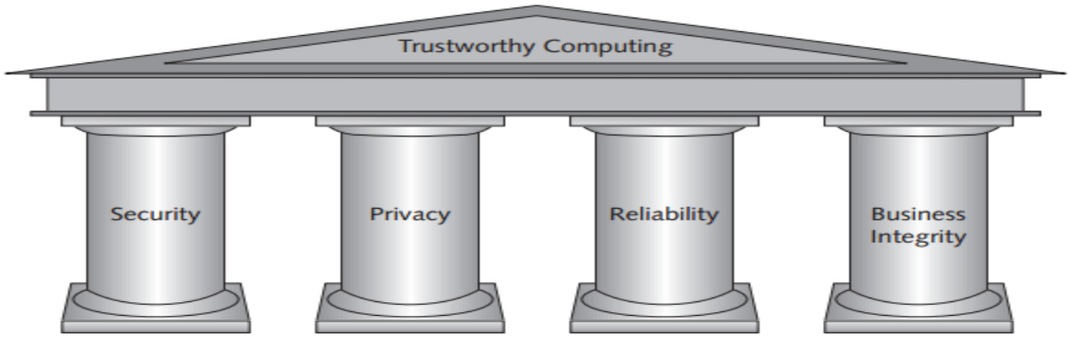


FIGURE Microsoft's Four Pillars of Trustworthy Computing

Pillar	Actions taken by Microsoft to support trustworthy computing
Security	Invest in the expertise and technology required to create a trustworthy environment. Work with law enforcement agencies, industry experts, academia, and private sectors to create and enforce secure computing. Develop trust by educating consumers on secure computing.
Privacy	Make privacy a priority in the design, development, and testing of products. Contribute to standards and policies created by industry organizations and government. Provide users with a sense of control over their personal information.
Reliability	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.
Business integrity	Be responsive—take responsibility for problems and take action to correct them. 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.

3.5 Risk Assessment:

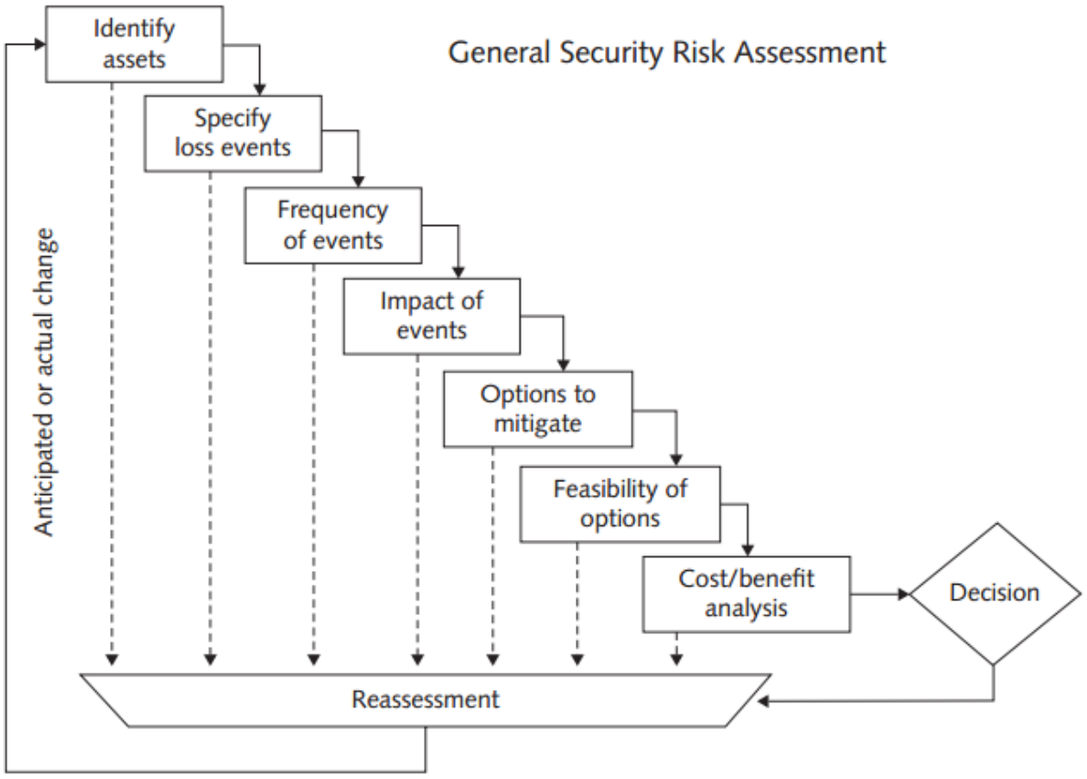
Q.What is risk assessment? w/13 IT

▪A risk assessment is the process of assessing security-related risks to an organization's computers and networks from both internal and external threats. Such threats can prevent an organization from meeting its key business objectives.

▪ 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.

▪ In the context of an IT risk assessment, an asset is any hardware, software, information system, network, or database that is used by the organization to achieve its business objectives.

▪A loss event is any occurrence that has a negative impact on an asset, such as a computer contracting a virus or a Web site undergoing a distributed denial-of-service attack



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

FIGURE General Security Risk Assessment

Step 1. Identify the set of IT assets about which the organization is most concerned. Priority is typically given to those assets that support the organization's mission and the meeting of its primary business goals.

Step 2.Identify the loss events or the risks or threats that could occur, such as a distributed denial-of-service attack or insider fraud.

Step 3. Assess the frequency of events or the likelihood of each potential threat; some threats, such as insider fraud, are more likely to occur than others.

Step 4.Determine the impact of each threat occurring. Would the threat have a minor impact on the organization, or could it keep the organization from carrying out its mission for a lengthy period of time?

Step 5.Determine how each threat can be mitigated so that it becomes much less

likely to occur or, if it does occur, has less of an impact on the organization. For example, installing virus protection on all computers makes it much less likely for a computer to contract a virus. Due to time and resource limitations, most organizations choose to focus on those threats that have a high (relative to all other threats) frequency and a high (relative to all other threats) impact. In other words, first address those threats that are likely to occur and that would have a high negative impact on the organization.

Step 6.Assess the feasibility of implementing the mitigation options.

Step 7.Perform a cost-benefit analysis to ensure that your efforts will be cost effective. No amount of resources can guarantee a perfect security system, so organizations must balance the risk of a security breach with the cost of preventing one. The concept of reasonable assurancerecognizes that managers must use their judgment to ensure that

the cost of control does not exceed the system's benefits or the risks involved.

Step 8.Make the decision on whether or not to implement a particular countermeasure. If you decide against implementing a particular countermeasure, you need to reassess if the threat is truly serious and, if so, identify a less costly countermeasure.

3.6 Prevention:

No organization can ever be completely secure from attack. The key is to implement a layered security solution to make computer break-ins so difficult that an attacker eventually gives up. In a layered solution, if an attacker breaks through one layer of security, there is another layer to overcome. These layers of protective measures are explained in more detail in the following sections.

3.6.1 Installing a Corporate Firewall:

Q. How does corporate firwall make computer break-ins difficult? S/14 IT

▪Installation of a corporate firewall is the most common security precaution taken by businesses.

▪ A firewall stands guard between an organization's internal network and the Internet, and it limits network access based on the organization's access policy Firewalls can be established through the use of software, hardware, or a combination of both.

▪Any Internet traffic that is not explicitly permitted into the internal network is denied entry. Similarly, most firewalls can be configured so that internal network users can be blocked from gaining access to certain Web sites based on such content as sex and violence.

▪Most firewalls can also be configured to block instant messaging, access to newsgroups, and other Internet activities

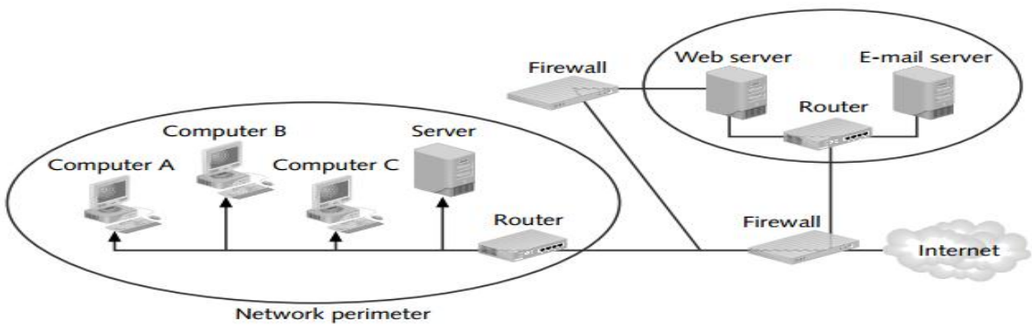


FIGURE Firewall

•Installing a firewall can lead to another serious security issue—complacency.

▪For example, a firewall cannot prevent a worm from entering the network as an e-mail attachment.

▪ Most firewalls are configured to allow e-mail and benign-looking attachments to reach their intended recipient.

3.6.2 Intrusion Prevention Systems

▪Intrusion prevention systems (IPSs)work to prevent an attack by blocking viruses, malformed packets, and other threats from getting into the protected network.

▪The IPS sits directly behind the firewall and examines all the traffic passing through it. A firewall and a network IPS are complementary.

▪Most firewalls can be configured to block everything except what you explicitly allow through; most IPSs can be configured to let through everything except what you explicitly specify should be blocked.

3.6.3 Installing Antivirus Software on Personal Computers

▪Antivirus software should be installed on each user's personal computer to scan a computer's memory and disk drives regularly for viruses.

▪ Antivirus software scans for a specific sequence of bytes, known as a virus signature, that indicates the presence of a specific virus.

▪If it finds a virus, the antivirus software informs the user, and it may clean, delete, or quarantine any files, directories, or disks affected by the malicious code.

▪Good antivirus software checks vital system files when the system is booted up, monitors the system continuously for virus-like activity, scans disks, scans memory when a program is run, checks programs when they are downloaded, and scans e-mail attachments before they are opened.

▪Two of the most widely used antivirus software products are Norton AntiVirus from Symantec and Personal Firewall from McAfee.

3.6.4 Implementing Safeguards Against Attacks by Malicious Insiders

▪User accounts that remain active after employees leave a company are potential security risks.

▪To reduce the threat of attack by malicious insiders, IT staff must promptly delete the computer accounts, login IDs, and passwords of departing employees and contractors.

▪ Organizations also need to define employee roles carefully and separate key responsibilities properly, so that a single person is not responsible for accomplishing a task that has high security implications.

▪For example, it would not make sense to allow an employee to initiate as well as approve purchase orders. That would allow an employee to input large invoices on behalf of a"friendly vendor,"approve the invoices for payment, and then disappear from the company to split the money with the vendor.

▪In addition to separating duties, many organizations frequently rotate people in sensitive positions to prevent potential insider crimes.

▪ Another important safeguard is to create roles and user accounts so that users have the authority to perform their responsibilities and nothing more.

▪ For example, members of the Finance Department should have different authorizations from members of Human Resources.

▪ An accountant should not be able to review the pay and attendance records of an employee, and a member of Human Resources should not know how much was spent to modernize a piece of equipment.

▪Even within one department, not all members should be given the same capabilities.

▪ Within the Finance Department, for example, some users may be able to approve invoices for payment, but others may only be able to enter them.

▪An effective administrator will identify the similarities among users and create profiles associated with these groups.

3.6.5 Addressing the Most Critical Internet Security Threats:

▪The overwhelming majority of successful computer attacks are made possible by taking advantage of well-known vulnerabilities. Computer attackers know that many organizations are slow to fix problems, which makes scanning the Internet for vulnerable systems an effective attack strategy.

▪The rampant and destructive spread of worms, such as Blaster, Slammer, and Code Red, was made possible by the exploitation of known but unpatched vulnerabilities.

▪Both the SANS (SysAdmin, Audit, Network, Security) Institute and US-CERT regularly update a summary of the most frequent, high-impact vulnerabilities being reported to them., respectively.

▪The actions required to address these issues include installing a known patch to the software, and keeping applications and operating systems up to date.

▪Those responsible for computer security must make it a priority to prevent attacks using these vulnerabilities.

3.7 Prevention of Cyber Attacks

Q. What are the ways of protecting an organization from different types of attack? W/14 CT

•You might already know that there is no 100% foolproof method to counter cybercrime and cyber attacks, but still, you have to take as many precautions to protect your computers.

•The primary things to be done are to use a good security software, that not only scans for virus, but also looks for different types of malware, including but not limited to ransom are, and stops it from entering the computer.

•Mostly these malicious codes are injected into your computers by visiting or downloading things from non-reputed websites, drive by downloads, compromised websites that display malicious advertisings also known as Malvertising.

•Along with the antivirus, you should use a good firewall.

•While the built in firewall in Windows 8 and Windows 7 is good, you can use third party firewalls that you feel are stronger than the default Windows Firewall.

•If it is a corporate computer network, make sure there is no Plug and Play support in any of the user computers.

•That is, employees should not be able to plug in Flash drives or their own Internet dongles into the USB. The IT department of the company should also keep a watch on all the network traffic.

•Using a good network traffic analyzer helps in prompt attendance to strange behaviors arising out of any terminal (employee computer).

•For protection against DDoS attacks, the website is better mitigated to different servers, instead of being hosted simply on a single server.

•The best method would be to have a mirror constantly up using a cloud service. That will greatly reduce the chances of a DDoS being successful – not for a long time at least. Use a good firewall like Sucuri and take some basic steps to protect and secure your website.

3.8 Conducting Periodic IT Security Audits

Q. State the purpose of an IT security audit and briefly discuss the key element of a such an audit S/14 CT

▪Another important prevention tool is a security audit that evaluates whether an organization has a well-considered security policy in place and if it is being followed.

▪For example, if a policy says that all users must change their passwords every 30 days, the audit must check how well the policy is being implemented.

▪The audit should also review who has access to particular systems and data and what level of authority each user has.

▪It is not unusual for an audit to reveal that too many people have access to critical data and that many people have capabilities beyond those needed to perform their jobs.

▪One result of a good audit is a list of items that need to be addressed in order to ensure that the security policy is being met.

▪A thorough security audit should also test system safeguards to ensure that they are operating as intended. Such tests might include trying the default system passwords that are active when software is first received from the vendor.

▪The goal of such a test is to ensure that all such known passwords have been changed. Some organizations will also perform a penetration test of their defenses.

▪This entails assigning individuals to try to break through the measures and identify vulnerabilities that still need to be addressed.

▪The individuals used for this test are often contractors rather than employees. The contractors may possess special skills or knowledge and are likely to take unique approaches in testing the security measures.

3.8 .1 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.

▪ Two fundamentally different approaches to intrusion detection are knowledge-based approaches and behavior-based approaches.

▪Knowledge-based intrusion detection systems contain information about specific attacks and system vulnerabilities, and watch for attempts to exploit these vulnerabilities, such as repeated failed login attempts or recurring attempts to download a program to a server.

▪ When such an attempt is detected, an alarm is triggered. A behavior based intrusion detection system models normal behavior of a system and its users from reference information collected by various means.

▪ The intrusion detection system compares current activity to this model and generates an alarm if it finds a deviation. Examples include unusual traffic at odd hours or a user in the Human Resources Department who accesses an accounting program that she has never before used.

3.8 . 2Response

▪An organization should be prepared for the worst—a successful attack that defeats all or some of a system's defenses and damages data and information systems.

▪ A response plan should be developed well in advance of any incident and be approved by both the organization's legal department and senior management.

▪A well-developed response plan helps keep an incident under technical and emotional control.

▪In a security incident, the primary goal must be to regain control and limit damage, not to attempt to monitor or catch an intruder.

▪ Sometimes system administrators take the discovery of an intruder as a personal challenge and lose valuable time that should be used to restore data and information systems to normal.

3.8 .3 Incident Notification

▪A key element of any response plan is to define who to notify and who not to notify.

▪Questions to cover include the following: Within the company, who needs to be notified, and what information does each person need to have? Under what conditions should the company contact major customers and suppliers? How does the company inform them of a disruption in business without unnecessarily alarming them? When should local authorities or the FBI be contacted?

▪Most security experts recommend against giving out specific information about a compromise in public forums, such as news reports, conferences, professional meetings, and online discussion groups.

▪ All parties working on the problem need to be kept informed and up to date without using systems connected to the compromised system. The intruder may be monitoring these systems and e-mail to learn what is known about the security breach.

3.8 .4 Protection of Evidence and Activity Logs:

▪An organization should document all details of a security incident as it works to resolve the incident.

▪Documentation captures valuable evidence for a future prosecution and provides data to help during the incident eradication and follow-up phases.

▪ It is especially important to capture all system events, the specific actions taken (what, when, and who), and all external conversations (what, when, and who) in a logbook.

▪ Because this may become court evidence, an organization should establish a set of document handling procedures using the legal department as a resource.

3.8 .5 Incident Containment

▪Often it is necessary to act quickly to contain an attack and to keep a bad situation from becoming even worse.

▪ The response plan should clearly define the process for deciding if an attack is dangerous enough to warrant shutting down or disconnecting critical systems from the network.

▪How such decisions are made, how fast they are made, and who makes them are all elements of an effective response plan

3.8 .6 Eradication

▪Before the IT security group begins the eradication effort, it must collect and log all possible criminal evidence from the system, and then verify that all necessary backups are current, complete, and free of any virus.

▪Creating a forensic disk image of each compromised system on write-only media both for later study and as evidence can be very useful.

▪After virus eradication, the group must create a new backup. Throughout this process, a log should be kept of all actions taken.

▪This will prove helpful during the follow-up phase and ensure that the problem does not recur. It is imperative to back up critical applications and data regularly.

▪Many organizations, however, have implemented inadequate backup processes and found that they could not fully restore original data after a security incident.

▪All backups should be created with enough frequency to enable a full and quick restoration of data if an attack destroys the original. This process should be tested to confirm that it works.

3.8 .7 Incident Follow-Up

▪ an essential part of follow-up is to determine how the organization's security was compromised so that it does not happen again. Often the fix is as simple as getting a software patch from a product vendor.

▪ However, it is important to look deeper than the immediate fix to discover why the incident occurred.

▪ If a simple software fix could have prevented the incident, then why wasn't the fix installed before the incident occurred? A review should be conducted after an incident to determine exactly what happened and to evaluate how the organization responded.

▪One approach is to write a formal incident report that includes a detailed chronology of events and the impact of the incident.

▪This report should identify any mistakes so that they are not repeated in the future. The experience from this incident should be used to update and revise the security incident response plan.

3.9

Q. Suggest security Training required for all employee in an IT organization W/13 S/14 CT

Empowering your employees to recognize common cyber threats can be beneficial to your organization's computer security. Security awareness training teaches employees to understand

vulnerabilities and threats to business operations. Your employees need to be aware of their responsibilities and accountabilities when using a computer on a business network.

New hire training and regularly scheduled refresher training courses should be established in order to instill the data security culture of your organization. Employee training should include, but not be limited to:

Responsibility for Company Data

Continually emphasize the critical nature of data security and the responsibility of each employee to protect company data. You and your employees have legal and regulatory obligations to respect and protect the privacy of information and its integrity and confidentiality.

Document Management and Notification Procedures

Employees should be educated on your data incident reporting procedure in the event an employee's computer becomes infected by a virus or is operating outside its norm (e.g., unexplained errors, running slowly, changes in desktop configurations, etc.). They should be trained to recognize a legitimate warning message or alert. In such cases, employees should immediately report the incident so your IT team can be engaged to mitigate and investigate the threat.

Passwords

Train your employees on how to select strong passwords. Passwords should be cryptic so they cannot be easily guessed but also should be easily remembered so they do not need to be in writing. Your company systems should be set to send out periodic automatic reminders to employees to change their passwords.

Unauthorized Software

Make your employees aware that they are not allowed to install unlicensed software on any company computer. Unlicensed software downloads could make your company susceptible to malicious software downloads that can attack and corrupt your company data.

Internet Use

Train your employees to avoid emailed or online links that are suspicious or from unknown sources. Such links can release malicious software, infect computers and steal company data. Your company also should establish safe browsing rules and limits on employee Internet usage in the workplace.

Email

Responsible email usage is the best defense for preventing data theft. Employees should be aware of scams and not respond to email they do not recognize. Educate your employees to accept email that:

- Comes from someone they know.
- Comes from someone they have received mail from before.
- Is something they were expecting.
- Does not look odd with unusual spellings or characters.
- Passes your anti-virus program test.

Social Engineering and Phishing

Train your employees to recognize common cybercrime and information security risks, including social engineering, online fraud, phishing and web-browsing risks.

Social Media Policy

Educate your employees on social media and communicate, at a minimum, your policy and guidance on the use of a company email address to register, post or receive social media.

Mobile Devices

Communicate your mobile device policy to your employees for company-owned and personally owned devices used during the course of business.

Protecting Computer Resources

Train your employees on safeguarding their computers from theft by locking them or keeping them in a secure place. Critical information should be backed up routinely, with backup copies being kept in a secure location. All of your employees are responsible for accepting current virus protection software updates on company PCs.

3.10

Q.Define Reliability with example W/13 W/14 CT

▪Reliability is an attribute of any computer-related component (software, or hardware, or a network, for example) that consistently performs according to its specifications.

▪It has long been considered one of three related attributes that must be considered when making, buying, or using a computer product or component.

▪Reliability, availability, and serviceability - RAS, for short - are considered to be important aspects to design into any system.

▪In theory, a reliable product is totally free of technical errors; in practice, however, vendors frequently express a product's reliability quotient as a percentage.

▪Evolutionary products (those that have evolved through numerous versions over a significant period of time) are usually considered to become increasingly reliable, since it is assumed that bug s have been eliminated in earlier releases.

▪For example, IBM's z/OS (an operating system for their S/390server series), has a reputation for reliability because it evolved from a long line of earlierMVS and OS/390 operating system versions.

3.11 Computer forensics

Q**. What is computer forensic? What role does it play in responding to computer incident? S/14 CSE**

Computer forensics

▪**Computer forensics** (sometimes known as **computer forensic science** is a branch of digital forensic science pertaining to illegal evidence found in computers and digital storage media.

▪The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information.

▪Although it is most often associated with the investigation of a wide variety of computer crime, computer forensics may also be used in civil proceedings.

▪The discipline involves similar techniques and principles to data recovery, but with additional guidelines and practices designed to create a legal audit trail.

▪Evidence from computer forensics investigations is usually subjected to the same guidelines and practices of other digital evidence.

▪ It has been used in a number of high-profile cases and is becoming widely accepted as reliable within U.S. and European court systems.

Use as evidence

▪In court, computer forensic evidence is subject to the usual requirements for digital evidence. This requires that information be authentic, reliably obtained, and admissible.

▪ Different countries have specific guidelines and practices for evidence recovery.

▪In the United Kingdom, examiners often follow Association of Chief Police Officers guidelines that help ensure the authenticity and integrity of evidence. While voluntary, the guidelines are widely accepted in British courts.

CHAPTER- 4

PRIVACY

4. PRIVACY PROTECTION AND THE LAW

‣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.

‣On the other hand, many people object to the data collection policies of government and business on the basis that they strip individuals of the power to control their own personal information.

‣For these people, the existing hodgepodge of privacy laws and practices fails to provide adequate protection; rather, it causes confusion that promotes distrust and skepticism, which are further fueled by the disclosure of threats to privacy, such as those detailed in the opening vignette on IRS systems.

‣ Indeed,"one of the key factors affecting the growth of e-commerce is the lack of Internet users' confidence in online information privacy."

‣A combination of approaches—new laws, technical solutions, and privacy policies—is required to balance the scales. Reasonable limits must be set on government and business access to personal information; new information and communication technologies must be designed to protect rather than diminish privacy; and appropriate corporate policies must be developed to set baseline standards for people's privacy.

4.1 Information Privacy:

Q. Describe issue in Information privacy w/13 ct
Q. Briefly describe the concept of right of privacy & Information privacy S/14 CT

‣**Information privacy**, or **data privacy (or data protection)**, is the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them.

‣Privacy concerns exist wherever personally identifiable information or other sensitive information is collected and stored – in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues.

‣Data privacy issues can arise in response to information from a wide range of sources, such as:

- Healthcare records
- Criminal justice investigations and proceedings
- Financial institutions and transactions
- Biological traits, such as genetic material
- Residence and geographic records
- Ethnicity
- Privacy breach
- Location-based service and geolocation

‣The challenge in data privacy is to share data while protecting personally identifiable information.

‣The fields of data security and information security design and utilize software, hardware and human resources to address this issue.

‣As the laws and regulations related to Data Protection are constantly changing, it is important to keep abreast of any changes in the law and continually reassess your compliance with data privacy and security regulations

4.2 Privacy Laws, Applications, and Court Rulings:

Financial Data

‣Individuals must reveal much of their personal financial data in order to take advantage of the wide range of financial products and services available, including credit cards, checking and savings accounts, loans, payroll direct deposit, and brokerage accounts.

‣To access many of these financial products and services, individuals must use a personal logon name, password, account number, or PIN.

‣The inadvertent loss or disclosure of this personal financial data carries a high risk of loss of privacy and potential financial loss. Individuals should be concerned about how this personal data is protected by businesses and other organizations and whether or not it is shared with other people or companies.

4.2.1 Fair Credit Reporting Act (1970)

‣The Fair Credit Reporting Actof 1970 regulates the operations of credit-reporting bureaus, including how they collect, store, and use credit information.

‣The act, enforced by the U.S. Federal Trade Commission, is designed to ensure the accuracy, fairness, and privacy of information gathered by the credit-reporting companies (such as

Experian, Equifax, and TransUnion) and to check those systems that gather and sell information about people.

‣The act outlines who may access your credit information, how you can find out what is in your file, how to dispute inaccurate data, how long data is retained, and so on. The manual procedures as well as the information systems of the credit-reporting bureaus must implement and support all of these regulations.

4.2.2 Gramm-Leach-Bliley Act (1999)

‣The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999, was a bank deregulation law that repealed a Depression-era law known as Glass-Steagall. Glass-Steagall prohibited any one institution from offering investment, commercial banking, and insurance services; individual companies were only allowed to offer one of those types of financial service products. GLBA enabled such entities to merge.

‣The emergence of new corporate conglomerates, such as Bank of America, Citigroup, and JPMorgan Chase, soon followed.

‣These one-stop financial supermarkets owned bank branches, sold insurance, bought and sold stocks and bonds, and engaged in mergers and acquisitions. Some place partial blame for the financial crisis that began in 2008 on the passage of GLBA and the loosening of banking restrictions.

4.2.3 Health Information

‣The use of electronic medical records and the subsequent interlinking and transferring of this electronic information among different organizations has become widespread.

‣Individuals are rightly concerned about the erosion of privacy of data concerning their health.

‣They fear intrusions into their health data by employers, schools, insurance firms, law enforcement agencies, and even marketing firms looking to promote their products and services. The primary law addressing these issues is the Health Insurance Portability and Accountability Act.

4.2.3.1 Health Insurance Portability and Accountability Act of 1996

‣The Health Insurance Portability and Accountability Act of 1996 (HIPAA)was designed to improve the portability and continuity of health insurance coverage; to reduce fraud, waste, and abuse in health insurance and healthcare delivery; and to simplify the administration of health insurance.

‣To these ends, HIPAA requires healthcare organizations to employ standardized electronic transactions, codes, and identifiers to enable them to fully digitize medical records, thus making it possible to exchange medical data over the Internet.

4.2.3.2 Children’s Personal Data

‣Internet use by children continues to climb; a recent report out of the United Kingdom found that teenagers spend an average of 31 hours per week online.

‣As a concerned society, many of us feel that there is a need to protect children from being exposed to inappropriate material and online predators; becoming the target of harassment; divulging personal data; and becoming involved in gambling or other inappropriate behavior.

‣To date, only a few laws have been implemented to protect children online, and most of these have been ruled unconstitutional under the First Amendment and its protection of freedom of expression.

4.2.3.3 Children's Online Privacy Protection Act (1998)

‣According to the Children's Online Privacy Protection Act (COPPA), any Web site that caters to children must offer comprehensive privacy policies, notify parents or guardians about its data-collection practices, and receive parental consent before collecting any personal information from children under 13 years of age.

‣ COPPA is meant to give parents control over the collection, use, and disclosure of their children's personal information; it does not cover the dissemination of information to children The law has had a major impact, requiring many companies to spend hundreds of thousands of dollars to make their sites compliant, while others eliminated preteens as a target audience.

4.2.4 Electronic Surveillance

This section covers laws that address government surveillance, including various forms of electronic surveillance. New laws have been added and old laws amended in recent years in reaction to worldwide terrorist activities and the development of new communication technologies

4.2.4.1 Communications Act of 1934

‣The Communications Act of 1934established the Federal Communications Commission and gave it responsibility for regulating all non-federal-government use of radio and television broadcasting and all interstate telecommunications—including wire, satellite, and cable—as well as all international communications that originate or terminate in the United States. The act also restricted the government's ability to secretly intercept communications.

4.2.4.2 Title III of the Omnibus Crime Control and Safe Streets Act (1968, amended 1986)

Title III of the Omnibus Crime Control and Safe Streets Act, also known as the Wiretap Act, regulates the interception of wire (telephone) and oral communications.

‣It allows state and federal law enforcement officials to use wiretapping and electronic eavesdropping, but only under strict limitations.

‣ Under this act, a warrant must be obtained from a judge to conduct a wiretap. The judge will approve the warrant only if" there is probable cause [to believe] that an individual is committing, has committed, or is about to commit a particular offense . . . [and that] normal investigative procedures have been tried and have failed or reasonably appear to be unlikely if tried or to be too dangerous

4.2.4.3 Foreign Intelligence Surveillance Act (1978)

‣The Foreign Intelligence Surveillance Act (FISA)of 1978 describes procedures for the electronic surveillance and collection of foreign intelligence information in communications between foreign powers and the agents of foreign powers.

‣Foreign intelligence is information relating to the capabilities, intentions, or activities of foreign governments or agents of foreign governments or foreign organizations.

‣The act allows surveillance, without court order, within the United States for up to a year unless the"surveillance will acquire the contents of any communication to which a U.S. person is a party."

4.3 KEY PRIVACY AND ANONYMITY ISSUES:

Q. What is right of privacy and what is the basis for protecting personal privacy under the law? W/13 CSE S/15 CT

4.3.1 Identity Theft

Q.What is identity theft and what technique do identity thieves use? S/14 W/14 IT W/13 S/14 , W/14 , S/15 CSE

‣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.

‣Using this information, an identity thief may apply for new credit or financial accounts, rent an apartment, set up utility or phone service, and register for college courses—all in someone else's name.

4.3.1.1 Data Breaches

An alarming number of identity theft incidents involve breaches of large databases to gain personal identity information. The breach may be caused by hackers breaking into the database or, more often than one would suspect, by carelessness or failure to follow proper security procedures.

4.3.1.2 Purchase of Personal Data

There is a black market in personal data. Credit card numbers can be purchased in bulk quantity for as little as $.40 each, while the logon name and PIN necessary to access a bank account can be had for just $10.

A full set of identity information—including date of birth, address, Social Security number, and telephone number—sells for between $1 and $15.

4.3.1.3 Phishing

phishing is an attempt to steal personal identity data by tricking users into entering information on a counterfeit Web site. Spoofed e-mails lead consumers to counterfeit Web sites designed to trick them into divulging personal data. Users have learned through sad experience that simply accessing a phishing Web site can trigger an automatic and transparent download of malware known as spyware to a computer.

4.3.1.4 Spyware

‣Spyware is keystroke-logging software downloaded to users' computers without the knowledge or consent of the user.

‣It is often marketed as a spouse monitor, child monitor, or surveillance tool. Spyware creates a record of the keystrokes entered on the computer, enabling the capture of account usernames, passwords, credit card numbers, and other sensitive information.

‣ The spy can view the Web sites visited as well as transcripts of chat logs. Spyware operates even if the infected computer is not connected to the Internet, continuing to record each keystroke until the next time the user connects to the Internet.

‣Then, the data captured by the spyware is e-mailed directly to the spy or is posted to a Web site where the spy can view it. Spyware frequently employs sophisticated methods to avoid detection by popular software packages that are specifically designed to combat it.

‣Consumers' fear of spyware has become so widespread that many people now delete e-mail from unknown sources without even opening the messages. This trend is seriously damaging the effectiveness of e-mail as a means for legitimate companies to communicate with customers.

4.3.1.5 Identity Theft Monitoring Services

‣There are numerous identity theft monitoring services, which offer a wide range of coverage.

‣‣Basic monitoring services cost about $10 per month and provide protection by monitoring the three major credit reporting agencies (TransUnion, Equifax, and Experian) for anyone using your personal data to apply for a new credit card, cell phone, or loan.

▪More expensive services monitor additional databases (e.g., financial institutions, utilities, and the DMV). Subscribers to these services receive a phone call or e-mail if suspicious activity is detected.

4.3.2 Consumer Profiling

Q. Discuss about consumer Profiling. W/13 W/14 , S/15 CT W/13 S/14 IT

‣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.
▪ The use of cookies and tracking software is controversial because companies can collect information about consumers without their explicit permission.

‣Outside of the Web environment, marketing firms employ similarly controversial means to collect information about people and their buying habits.

▪Each time a consumer uses a credit card, redeems frequent flyer points, fills out a warranty card, answers a phone survey, buys groceries using a store loyalty card, orders from a mail-order catalog, or registers a car with the DMV, the data is added to a storehouse of personal information about that consumer, which may be sold or shared with third parties.

‣ In many of these cases, consumers never explicitly consent to submitting their information to a marketing organization.

4.3.3 Aggregating Consumer Data

▪Marketing firms aggregate the information they gather about consumers to build databases that contain a huge amount of consumer data.

▪They want to know as much as they can about consumers—who they are, what they like, how they behave, and what motivates them to buy. The marketing firms provide this data to companies so that they can tailor their products and services to individual consumer preferences.

▪Advertisers use the data to more effectively target and attract customers to their messages. Ideally, this means that buyers should be able to shop more efficiently and find products that are well suited for them.

▪Sellers should be better able to tailor their products and services to meet their customers' desires and to increase sales.

▪However, concerns about how all this data is actually used is a major reason why many potential Web shoppers have not yet made online purchases.

4.3.3 .1 Collecting Data from Web Site Visits

‣Marketers use cookies to recognize return visitors to their sites and to store useful information about them. The goal is to provide customized service for each consumer.

‣ When someone visits a Web site, the site asks that person's computer if it can store a cookie on the hard drive.

‣If the computer agrees, it is assigned a unique identifier, and a cookie with this identification number is placed on its hard drive. Cookies allow marketers to collect click stream data—information gathered by monitoring a consumer's online activity. During a Web-surfing session, three types of data are gathered.

‣First, as one browses the Web,"GET" data is collected. GET data reveals, for example, that the consumer visited an affiliated book site and requested information about the latest Dean Koontz book.

‣Second,"POST"data is captured. POST data is entered into blank fields on an affiliated Web page when a consumer signs up for a service, such as the Travelocity service that sends an e-mail when airplane fares change for flights to favorite destinations.

‣Third, the marketer monitors the consumer's surfing throughout any affiliated Web sites, keeping track of the information the user sought and viewed. Thus, as a person surfs the Web, a tremendous amount of data is generated for marketers and sellers.

4.3.3 .2 Personalization Software

Q. Why personalization S/W are used? What are different types of personalization S/W. **W/14 IT**

‣In addition to using cookies to track consumer data, online marketers use personalization software to optimize the number, frequency, and mixture of their ad placements, and to evaluate how visitors react to new ads.

‣The goal is to turn first-time visitors to a site into paying customers and to facilitate greater cross-selling activities.

‣There are several types of personalization software. For example, rules-based personalization software uses business rules tied to customer-supplied preferences or online behavior to determine the most appropriate page views and product information to display when a user visits a Web site.

‣ For instance, if you use a Web site to book airline tickets to a popular vacation spot, rules based software might ensure that you are shown ads for rental cars.

▪Collaborative filtering offers consumer recommendations based on the types of products purchased by other people with similar buying habits. For example, if you bought a book by Dean Koontz, a company might recommend Stephen King books to you, based on the fact that a significant percentage of other customers bought books by both authors.

▪Demographic filtering is another form of personalization software. It augments clickstream data and user-supplied data with demographic information associated with user zip codes to make product suggestions.

▪Microsoft has captured age, sex, and location information for years through its various Web sites, including MSN and Hotmail.

▪ It has accumulated a vast database on tens of millions of people, each assigned a global user ID. Microsoft has also developed a technology based on this database that enables marketers to target one ad to men and another to women.

▪ Additional information such as age and location can be used as ad-selection criteria.

▪Yet another form of personalization software, contextual commerce, associates product promotions and other e-commerce offerings with specific content a user may receive in a news story online. For example, as you read a story about white-water rafting, you may be offered a deal on rafting gear or a promotion for a white-water rafting vacation in West Virginia.

▪ Instead of simply bombarding customers at every turn with standard sales promotions that result in tiny response rates, marketers are getting smarter about where and how they use personalization. They are also taking great care to measure whether personalization is paying off.

▪The intended result is that effective personalization increases online sales and improves consumer relationships.

▪Online marketers cannot capture personal information, such as names, addresses, and Social Security numbers, unless people provide them. Without this information, companies can't contact individual Web surfers who visit their sites.

▪ Data gathered about a user's Web browsing through the use of cookies is anonymous, as long as the network advertiser doesn't link the data with personal information. However, if a Web site visitor volunteers personal information, a Web site operator can use it to find additional personal information that the visitor may not want to disclose.

▪For example, a name and address can be used to find a corresponding phone number, which can then lead to obtaining even more personal data.

▪All this information becomes extremely valuable to the Web site operator, who is trying to build a relationship with Web site visitors and turn them into customers. The operator can use this data to initiate contact or sell it to other organizations with which they have marketing agreements.

4.3.3 .3 Consumer Data Privacy

▪Consumer data privacy has grown into a major marketing issue. Companies that can't protect or don't respect customer information often lose business and some become defendants in class action lawsuits stemming from privacy violations.

▪ For example, privacy groups spoke out vigorously to protest the proposed merger of Web ad server Double Click and database marketing company Abacus Direct.

▪ The groups were concerned that the information stored in cookies would be combined with data from mailing lists, thus revealing the Web users' identities. This would enable a network advertiser to identify and track the habits of unsuspecting consumers.

4.3.4 Treating Consumer Data Responsibly

Q. What must organization do to treat Consumer Data Responsibly? W/14 CSE

▪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 1980 OECD 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

4.3.5 Workplace Monitoring

Q. Why and how are employers increasingly using workplace monitoring? W/14 IT W/13, S/15 CSE

▪**Workplace monitoring** is the act of monitoring employee activity. Organizations engage in employee monitoring to track performance, avoid legal liability, protect trade secrets, and address other security concerns.

▪The practice may impactemployee satisfaction due to its impact on privacy.

▪The workplace in order to protect against employee abuses that reduce worker productivity or expose the employer to harassment lawsuits.

▪For example, an employee may sue his or her employer for creating an environment conducive to sexual harassment if other employees are viewing pornography online while at work and the organization takes no measures to stop such viewing. (E-mail containing crude jokes and cartoons or messages that discriminate against others based on sex, race, or national origin can also spawn lawsuits.)

▪The institution and communication of an IT usage policy establishes boundaries of acceptable behavior and enables management to take action against violators the extent of workplace monitoring.

▪The potential for decreased productivity, coupled with increased legal liabilities from computer users, have led employers to monitor workers to ensure that the corporate IT usage policy is followed.

▪ Many major U.S. firms find it necessary to record and review employee communications and activities on the job, including phone calls, e-mail, Internet connections, and computer files.

▪ Some are even videotaping employees on the job. In addition, some companies employ random drug testing and psychological testing. With few exceptions, these increasingly common (and many would say intrusive) practices are perfectly legal.

4.3.6 Electronic discovery

Q. What do you understand by an e-discovery? W/13 w/14 CT

▪**Electronic discovery** (or *e-discovery* or *ediscovery*) refers to discovery in litigation or government investigations which deals with the exchange of information in electronic format (often referred to as electronically stored information or ESI).

▪ These data are subject to local rules and agreed-upon processes, and are often reviewed for privilege and relevance before being turned over to opposing counsel.

▪Data are identified as potentially relevant by attorneys and placed on legal hold. Evidence is then extracted and analyzed using digital forensic procedures, and is reviewed using a document review platform.

▪Documents can be reviewed either as native files or after a conversion to PDF or TIFF form.

▪ A document review platform is useful for its ability to aggregate and search large quantities of ESI.

▪Electronic information is considered different from paper information because of its intangible form, volume, transience and persistence

4.3.7 Advanced Surveillance Technology:

Q. Describe advanced surveillance Technology S/14, W/14 CT

▪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.

▪Advocates of advanced surveillance technology argue that people have no legitimate expectation of privacy in a public place.

▪Critics raise concerns about the use of surveillance to secretly store images of people, creating a new potential for abuse, such as intimidation of political dissenters or blackmail of people caught with the"wrong"person or in the "wrong"place.

▪Critics also raise the possibility that such technology may not identify people accurately.

4.3.7.1 Camera Surveillance

A smart surveillance system, which singles out people who are acting suspiciously, is under development in Australia. In a smart surveillance system, computers learn what "normal"behavior is and then look for patterns of behavior outside the norm. When the system detects unusual behavior, it alerts authorities so that they can take preemptive action..

4.3.7.2 GPS Chips

▪From automobiles to cell phones, Global Positioning System (GPS) chips are being placed in many devices to precisely locate users.

▪The FCC has asked cell phone companies to implement methods for locating users so that police, fire, and medical personnel can be accurately dispatched to assist 911 callers.

▪ Similar location-tracking technology is also available for personal digital assistants, laptop computers, trucks, and boats. Parents can place one of these chips in their teenager's car, then use software to track the car's whereabouts.

▪Banks, retailers, and airlines are eager to gain real-time access to consumer location data, and have already devised a number of new services they want to provide—sending digital coupons for stores that particular consumers are near, providing the location of the nearest ATM, and updating travelers on flight and hotel information.

▪Airlines are considering the use of wireless devices both to enable passengers to check in for flights when they are close to the gate, and to monitor when each person passes through the gate.

▪Businesses claim that they will respect the privacy of wireless users and allow them to opt in or opt out of marketing programs that are based on their location data.

▪Wireless spamming is a distinct possibility—a user might continuously receive wireless ads, notices for local restaurants, and shopping advice while walking down the street.

▪ Another concern is that the data could be used to track people down at any time or to figure out where they were at some particular instant. The potential to reveal one's location when using a cell phone might cause some people to reconsider using one in the future.

Q. What are recommendations for safeguarding identity data? W/13 IT

1. Shred All Identifying Documents, Bank Slips, Etc.

Bank deposit receipts, credit card statements, old documents, anything with sensitive information should be properly disposed of. If you don't have a fireplace, consider investing in a low-cost paper shredder. Identity thieves can learn a lot from rifling through trash -- don't let yours give away your identity.

2. Shop Online Only on Secure Web Sites

Shopping online is safe -- when you use secure web pages. Check the bottom of your browser and look for a locked graphic, or look for "https" in the address bar. This means you are on a secure web page and your data is encrypted. Without a secure connection, hackers can eavesdrop on your transaction and grab your private data.

3. Don't Fall for Phishing Scams

Phishing is a technique employed by identity thieves through email or online chat services. The thief pretends to represent a company, such as PayPal or your credit card issuer, and informs you that you need to respond with some information or click on a link. The thief may even claim to represent a charity or sweepstakes giveaway. Don't fall for it. Don't respond and don't click the link, even if it *appears* to be a legitimate link. Responsible organizations will not contact you in this way.

4. Beware of Telephone Scams

Never give out personal information over the phone to someone who calls you claiming to represent a bank, credit card company, charity, or other organization. People are not always who they claim to be. You could be talking to a scam artist who is sweet-talking you out of your credit card or bank account number. This is an old scam, but still widely practiced today because it works. Don't let it work on you.

5. Keep Anti-Virus and Anti-Spyware Software Up to Date

A computer virus or trojan horse spyware program that sneaks its way onto your computer can compromise your private information. These malicious programs can scan through your entire

harddrive and send what it finds out over the internet. To combat this threat, be sure to run an anti-virus program and at least one anti-spyware program, such as Lavasoft's Ad-Aware. These programs will help defend your computer against those who want to compromise it.

6. Check Your Credit Report

According to US law every citizen is entitled to one free credit report each year. You can get the free report from the three major credit agencies by going to Annualcreditreport.com. Verify that the information is correct and check for suspicious activity, particularly mysterious new accounts opened. For even better protection, sign up for a service that notifies you when changes occur to your credit report.

7. Ask About Identity Theft Prevention Procedures

Ask your bank about what they are doing to combat identity theft. Call your credit card company and find out if you will be liable for fraudulent charges. Ask your employer about what steps are taken to safeguard sensitive employee data. It's your data; you should know how it is managed.

8. Secure Your Important Documents

Your social security card, passport, birth certificate and other identifying materials are highly sought-after by identity thieves and can command top dollar on the black market. Be sure that your documents are safely stored, preferably in a locked box tucked away and out of sight. Do not regularly carry these documents on you. When you travel, pay special attention to securing your passport. Leave it in a hotel room safe at all times.

9. Be Vigilant About Your Social Security Number

Some institutions--insurers, colleges, etc.--prefer to use your social security number as their identification number for you. This is very foolish, as it essentially deprivatizes this number. Because your social security number can be used to gain access to a lot of other private information about you, opt out of allowing institutions to use it. Another number can be substituted instead.

10. Be Careful With Your Mail

Of course tampering with someone's mail is a federal offense, but that doesn't stop people from doing it. Try not to let incoming mail sit in your mailbox for a long time. If you are going to be away, have the post office hold your mail for you. When sending out sensitive mail, consider dropping it off at a secure collection box or at the post office itself.

CHAPTER 5
FREEDOM OF EXPRESSION

5. Freedom of expression:

Q.What is the basis for freedom of expression for protection ? S/15 CT

Q. What is the basis for the protection of freedom of expression in united state? What types of

•The Internet enables a worldwide exchange of news, ideas, opinions, rumors, and information. Its broad accessibility, open discussions, and anonymity make the Internet a remarkable communications medium.

• It provides an easy and inexpensive way for a speaker to send a message to a large audience, potentially thousands of people worldwide.

•In addition, given the right e-mail addresses, a speaker can aim a message with laser accuracy at a select subset of powerful and influential people.

•People must often make ethical decisions about how to use such incredible freedom and power. Organizations and governments have attempted to establish policies and laws to help guide people, as well as to protect their own interests.

•Businesses, in particular, have sought to conserve corporate network capacity, avoid legal liability, and improve worker productivity by limiting the non-business use of IT resources.

•The right to freedom of expression is one of the most important rights for free people everywhere. The First Amendment to the U.S. Constitution was adopted to guarantee this right and others.

•Over the years, a number of federal, state, and local laws have been found unconstitutional because they violated one of the tenets of this amendment.

•In other words, the First Amendment protects Americans' rights to freedom of religion and freedom of expression. This amendment has been interpreted by the Supreme Court as applying to the entire federal government, even though it only expressly refers to Congress.

Numerous court decisions have broadened the definition of speech to include nonverbal, visual, and symbolic forms of expression, such as flag burning, dance movements, and hand gestures

•. Sometimes the speech at issue is unpopular or highly offensive to a majority of people; however, the Bill of Rights provides protection for minority views. The Supreme Court has also ruled that the First Amendment protects the right to speak anonymously as part of the guarantee of free speech.

▪**However, the Supreme Court has held that the following types of speech are not protected by the First Amendment and may be forbidden by the government: perjury, fraud, defamation, obscene speech, incitement of panic, incitement to crime,"fighting words,"and sedition** (incitement of discontent or rebellion against a government).

▪ Two of these types of speech—obscene speech and defamation—are particularly relevant to information technology.

FOR INDIVIDUALS

At an individual level, freedom of expression is key to the development, dignity and fulfillment of every person.

- People can gain an understanding of their surroundings and the wider world by exchanging ideas and information freely with others. This makes them more able to plan their lives and to work

- People feel more secure and respected by the state if they are able to speak their minds.

FOR STATES

At a national level, freedom of expression is necessary for good government and therefore for economic and social progress.

Freedom of expression and freedom of information contribute to the quality of government in various ways:

1. They help ensure that competent and honest people administer the state. In a democracy, free debate about and between political parties exposes their strengths and weaknesses. This enables voters to form an opinion about who is best qualified to run the country and to vote accordingly. Media scrutiny of the government and the opposition helps expose corruption or other improprieties and prevents a culture of dishonesty

2. They promote good governance by enabling citizens to raise their concerns with the authorities. If people can speak their minds without fear, and the media are allowed to report what is being said, the government can become aware of any concerns and address them.

3. They ensure that new policies and legislation are carefully considered. Through public debate, members of the public with helpful opinions on a subject can present the government with a 'marketplace of ideas' from which to choose. Free debate about new legislation also helps ensure that the eventual law has the support of the population, making it more likely to be respected.

4. They promote the implementation of other human rights. They help improve government policy in all areas, including human rights. They also enable journalists and activists to highlight human rights issues and abuses and persuade the government to take action.

5.1 FIRST AMENDMENT RIGHT:

Q. State first First Amendment Right W/13 IT W/14 CT

‣The Internet enables a worldwide exchange of news, ideas, opinions, rumors, and information. Its broad accessibility, open discussions, and anonymity make the Internet a remarkable communications medium.

‣It provides an easy and inexpensive way for a speaker to send a message to a large audience, potentially thousands of people worldwide.

‣In addition, given the right e-mail addresses, a speaker can aim a message with laser accuracy at a select subset of powerful and influential people.

‣People must often make ethical decisions about how to use such incredible freedom and power.

‣Organizations and governments have attempted to establish policies and laws to help guide people, as well as to protect their own interests. Businesses, in particular, have sought to conserve corporate network capacity, avoid legal liability, and improve worker productivity by limiting the non-business use of IT resources.

‣The right to freedom of expression is one of the most important rights for free people everywhere. The First Amendment to the U.S. Constitution was adopted to guarantee this right

and others. Over the years, a number of federal, state, and local laws have been found unconstitutional because they violated one of the tenets of this amendment.

5.1.1 Obscene Speech:

‣Miller v. Californiais the 1973 Supreme Court case that established a test to determine if material is obscene and therefore not protected by the First Amendment. Marvin Miller, after conducting a mass mailing campaign to advertise the sale of adult material, was convicted of violating a California statute prohibiting the distribution of obscene material.

‣ Some unwilling recipients of Miller's brochures complained to the police, initiating the legal proceedings. Although the brochures contained some descriptive printed material, they primarily consisted of pictures and drawings explicitly depicting men and women engaged in sexual activity.

5.1.2 Defamation:

‣The right to freedom of expression is restricted when the expressions, whether spoken or written, are untrue and cause harm to another person.

‣Making either an oral or a written statement of alleged fact that is false and that harms another person is defamation.

‣The harm is often of a financial nature, in that it reduces a person's ability to earn a living, work in a profession, or run for an elected office.

‣An oral defamatory statement is slander, and a written defamatory statement is libel.

‣Because defamation is defined as an untrue statement of fact, truth is an absolute defense against a charge of defamation.

‣ Although people have the right to express opinions, they must exercise care in their online communications to avoid possible charges of defamation.

‣Organizations must also be on their guard and prepared to take action in the event of libelous attacks against them.

5.2 FREEDOM OF EXPRESSION: KEY ISSUES

Q. What are the issue in freedom of expression ? W/13 , S/14 CT W/13, S/14 CSE

Controlling Access to Information on the Internet

Q. What are some key fedral laws that affect online freedom of expression & how do they impact organization? S/14 CSE

Q. How to control access to information on the internet? W/14 CSE

Although there are clear and convincing arguments to support freedom of speech online, the issue is complicated by the ease with which children can access the Internet. Even some advocates of free speech acknowledge the need to restrict children's Internet access, but it is difficult to restrict their access without also restricting adults' access. In attempts to address this issue, the U.S. government has passed laws, and software manufacturers have invented special software to block access to objectionable material. The following sections summarize these approaches.

5.2.1 Communications Decency Act (CDA) (1996):

‣The Telecommunications Act became law in 1996. Its purpose was to allow freer competition among phone, cable, and TV companies. Embedded in the Telecommunications Act was the Communications Decency Act (CDA), aimed at protecting children from pornography.

‣The CDA imposed $250,000 fines and prison terms of up to two years for the transmission of“indecent”material over the Internet.

.

5.2.1.1 Child Online Protection Act (COPA) (1998)

‣In October 1998, the Child Online Protection Act (COPA)was signed into law. (This act is not to be confused with the Children’s Online Privacy Protection Act [COPPA],

‣The law states that“who ever knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web, makes any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors shall be fined not more than $50,000, imprisoned not more than 6 months, or both.

‣The law became a significant battleground for proponents of free speech.

‣it affect sellers of explicit material online and their potential customers, but it could ultimately set standards for Internet free speech. Supporters of COPA (primarily the Department of Justice) argued that the act protected children from online pornography while preserving the rights of adults.

5.2.1.2 Internet Filtering:

Q. Different types of Internet filtering S/15 CT

‣An Internet filter is software that can be used to block access to certain Web sites that contain material deemed inappropriate or offensive.

‣The best Internet filters use a combination of URL, keyword, and dynamic content filtering. With URL filtering, a particular URL or domain name is identified as belonging to an objectionable site, and the user is not allowed access to it.

‣Keyword filtering uses keywords or phrases—such as sex, Satan, and gambling—to block Web sites. With dynamic content filtering, each Web site’s content is evaluated immediately before it is displayed, using such techniques as object analysis and image recognition.

‣Organizations may direct their network administrators to install filters on employees’ computers to prevent them from viewing sites that contain pornography or other objectionable material.

‣Employees who are unwillingly exposed to such material would have a strong case for sexual harassment.

‣The use of filters can also ensure that employees do not waste their time viewing non-business-related Web sites.

5.2.1.2 .1 Types of Internet Filters

Whether to protect children from inappropriate content or keep employees productive, Internet filters can help. As the name suggests, Internet filters restrict unwanted, inappropriate and possibly harmful content. While they all serve the same basic function, there are different types to choose from, making knowing the differences crucial to forming an informed decision.

Client-Side vs. Server-Side

- Client-side filtering is installed directly onto the PC like any other software program. From there, it monitors Internet activity, blocking inappropriate content. Both home users and businesses can use client-side Internet filtering. Server-side filtering typically resides on the company server,

controlling access for all connected computers. BusinessFilters.com warns that server-side filtering isn't very customizable, making a client-side solution more viable. While both may utilize the same blocking or filtering tactics, client-side software typically has more customization, a broader feature set and more frequent updates.

Black & White List Filters

- Blacklist filtering, according to Geeks.com, is one of the more popular methods, because of its ease of use. This type of software requires the parent or administrator to manually enter websites deemed inappropriate. After the website is recorded by the software, further access will be denied. White list filters use the same principle, just in reverse. This much-stricter method requires the parent or administrator to specify websites that can be accessed instead of ones that can't. In other words, this method filters out the majority of the Internet, allowing access only to specifically pre-determined websites.

Keyword and Content Filters

- Keyword and content filtering software takes a similar approach to black and white list filters, only filtering out websites with specific words or pre-defined content. For example, a home Internet filter might offer to filter out pornographic content. The software will then try to determine, through the words used on the site and previously databased information, whether a specific site is pornographic. If so, the user will be denied. According to Geeks.com, this method is often ineffective, because it tends to block legitimate websites misinterpreted as inappropriate. Conversely, if the keyword or content filter is set too low, it may allow unwanted content through, unable to recognize the site for what it is.

5.2.1.3 Children's Internet Protection Act (CIPA) (2000):

Q. Short note on Children's Internet Protection Act W/13 IT

‣In another attempt to protect children from accessing pornography and other explicit material online, Congress passed the Children's Internet Protection Act (CIPA)in 2000.

‣The act required federally financed schools and libraries to use some form of technological protection (such as an Internet filter) to block computer access to obscene material, pornography, and anything else considered harmful to minors.

‣ Congress did not specifically define which content or Web sites should be forbidden or which measures should be used—these decisions were left to individual school districts and library systems.

‣Any school or library that failed to comply with the law would no longer be eligible to receive federal money through the E-Rate program, which provides funding to help pay for the cost of Internet connections.

The following points summarize CIPA:]

‣Opponents of the law were concerned that it transferred power over education to

private software companies who develop the Internet filters and define which sites to block.

‣Furthermore, opponents felt that the motives of these companies were unclear—for example, some filtering companies track students' Web-surfing activities and sell the data to market research firms.

‣Opponents also pointed out that some versions of these filters were ineffective, blocking access to legitimate sites and allowing access to objectionable ones.

‣Yet another objection was that penalties associated with the act could cause schools and libraries to lose federal funds from the E-Rate program, which is intended to help bridge the digital divide between rich and poor, urban and rural.

‣Loss of federal funds would lead to a less capable version of the Internet for students at poorer schools, which have the fewest alternatives to federal aid.

‣CIPA's proponents contended that shielding children from drugs, hate, pornography, and other topics was a sufficient reason to justify filters.

‣They argued that Internet filters are highly flexible and customizable, and that critics exaggerated the limitations.

‣Proponents pointed out that schools and libraries could elect not to implement a children's Internet protection program; they just wouldn't receive federal money for Internet access.

5.2.1.4 Anonymity on the Internet

Q. Short Note on Anonymity on the Internet S/14 IT S/15 CSE

‣Anonymous expression is the expression of opinions by people who do not reveal their identity.

‣ The freedom to express an opinion without fear of reprisal is an important right of a democratic society.

‣Anonymity is even more important in countries that don't allow free speech. However, in the wrong hands, anonymous communication can be used as a tool to commit illegal or unethical activities.

‣Maintaining anonymity on the Internet is important to some computer users.

‣They might be seeking help in an online support group, reporting defects about a manufacturer's goods or services, taking part in frank discussions of sensitive topics, expressing a minority or antigovernment opinion in a hostile political environment, or participating in chat rooms.

‣Other Internet users would like to ban Web anonymity because they think that its use increases the risks of defamation, fraud, libel, and the exploitation of children.

‣When data is sent over the Internet, a computer's IP address (a numeric identification for a computer attached to the Internet) is logged by the ISP.

‣ The IP address can be used to identify the sender of an e-mail or an online posting. Internet users who want to remain anonymous can send e-mail to an anonymous remailer service, which uses a computer program to strip the originating IP number from the message.

‣It then forwards the message to its intended recipient—an individual, a chat room, or a newsgroup—with either no IP address or a fictitious one. This ensures that no header information can identify the author.

‣Some remailers route messages through multiple remailers to provide a virtually untraceable level of anonymity.

‣The use of a remailer keeps communications anonymous; what is communicated, and whether it is ethical or legal, is up to the sender.

‣The use of remailers by people committing unethical or even illegal acts in some states or countries has spurred controversy.

‣Remailers are frequently used to send pornography, to illegally post copyrighted material to Usenet newsgroups, and to send unsolicited advertising to broad audiences (spamming). An organization's IT department can set up a firewall to prohibit employees from accessing remailers or to send a warning message each time an employee communicates with a remailer

5.2.1.5 Defamation and Hate Speech:

Q. Short Note on Defamation & Hate speech W/13, S/14 IT S/15 CSE

Defamation

‣**Defamation—**is the communication of a false statement that harms the reputation of an individual person, business, product, group, government, religion, or nation as well as other various kinds of defamation that retaliate against groundless criticism.

‣Under common law, to constitute defamation, a claim must generally be false and have been made to someone other than the person defamed.

‣Some common law jurisdictions also distinguish between spoken defamation, called **slander**, and defamation in other media such as printed words or images, called **libel**.

‣False light laws protect against statements which are not technically false but misleading

‣In some civil law jurisdictions, defamation is treated as a crime rather than a civil wrong. The United Nations Commission on Human Rights ruled in 2012 that the criminalization of libel violates freedom of expression and is inconsistent with Article 19 of the International Covenant on Civil and Political Rights.

‣A person who defames another may be called a "defamer", "famacide", "libeler" or "slanderer

Hate speech

‣**Hate speech** is, outside the law, speech that attacks a person or group on the basis of attributes such as gender, ethnic origin, religion, race, disability, or sexual orientation.

‣In law, hate speech is any speech, gesture or conduct, writing, or display which is forbidden because it may incite violence or prejudicial action against or by a protected individual or group, or because it disparages or intimidates a protected individual or group.

‣The law may identify a protected individual or a protected group by certain characteristics. In some countries, a victim of hate speech may seek redress under civil law, criminal law, or both. A website that uses hate speech is called a *hate site*.

‣Most of these sites contain Internet forums and news briefs that emphasize a particular viewpoint.

‣There has been debate over how freedom of speech applies to the Internet as well as hate speech in general.

‣Critics have argued that the term "hate speech" is a contemporary example of Newspeak, used to silence critics of social policies that have been poorly implemented in a rush to appear politically correct.

5.2.1.6 Corporate blog

Q. Short note on Corporate blog S/14 IT,. W/14 CT W/14 CSE S/15 CSE

‣**Corporate blog** is a blog that is published and used by an organization, corporation, etc. to reach its organizational goals. The advantage of blogs is that posts and comments are easy to reach and follow due to centralized hosting and generally structured conversation threads.

‣Although there are many different types of corporate blogs, most can be categorized as either external or internal.

Types of corporate blogs

Internal blogs

An internal blog, generally accessed through the corporation's Intranet, is a weblog that any employee can view. Many blogs are also communal, allowing anyone to post to them. The informal nature of blogs may encourage:

- employee participation
- free discussion of issues
- collective intelligence
- direct communication between various layers of an organization
- a sense of community

Internal blogs may be used in lieu of meetings and **e-mail discussions**, and can be especially useful when the people involved are in different locations, or have conflicting schedules. Blogs may also allow individuals who otherwise would not have been aware of or invited to participate in a discussion to contribute their expertise.

External blogs

▪An external blog is a publicly available weblog where company employees, teams, or spokespersons share their views.

▪ It is often used to announce new products and services (or the end of old products), to explain and clarify policies, or to react on public criticism on certain issues.

▪It also allows a window to the company culture and is often treated more informally than traditional press releases, though a corporate blog often tries to accomplish similar goals as press releases do.

▪In some corporate blogs, all posts go through a review before they are posted. Some corporate blogs, but not all, allow comments to be made to the posts. According to Hoffman Agency, corporate blogs should not be 'about me', but should be a platform to show thought leadership and communicate views on industry issues.

▪External corporate blogs, by their very nature, are biased, though they can also offer a more honest and direct view than traditional communication channels. Nevertheless, they remain public relations tools.

▪Corporate blogs may be written primarily for consumers (Business-to-consumer) or primarily for other businesses (B2b).

▪Certain corporate blogs have a very high number of subscribers. The official Google Blog is currently in the Technorati top 50 listing among all blogs worldwide.

▪ The number of subscribers, blog comments, links to blog posts, and the number of times a post is shared in other social media are indicators of a blog's popularity, potential influence, and reach.

▪While business blogs targeted to consumer readers may have a high number of subscribers, comments, and other measures of engagement; corporate blogs targeted to other businesses, especially those in niche industries, may have a very limited number of subscribers, comments, links, and sharing via social media. Accordingly, other metrics are often evaluated to determine the success and effectiveness of B2B blogs.

▪Marketers might expect to have product evangelists or influencers among the audience of an external blog. Once they find them, they may treat them like VIPs, asking them for feedback on exclusive previews, product testing, marketing plans, customer services audits, etc.

▪The business blog can provide additional value by adding a level of credibility that is often unobtainable from a standard corporate site.

5.2.1.7 Pornography

• Many people, including some free-speech advocates, believe that there is nothing illegal or wrong about purchasing adult pornographic material made by and for consenting adults

▪The Internet has been a boon to the pornography industry by providing fast, cheap, and convenient access to well over 4.2 million porn Web sites worldwide. Access via the Internet enables pornography consumers to avoid offending others or being embarrassed

▪**Pornography** is the portrayal of sexual subject matter for the purpose of sexual arousal. Pornography may be presented in a variety of media, including books, magazines, postcards, photographs, sculpture, drawing, painting, animation, sound recording, film, video, and video games.

▪The term applies to the depiction of the act rather than the act itself, and so does not include live exhibitions like sex shows and striptease.

▪The primary subjects of pornographic depictions are pornographic models, who pose for still photographs, and pornographic actors or porn stars, who perform in pornographic films.

▪ If dramatic skills are not involved, a performer in a porn film may also be called a model.

▪Various groups within society have considered depictions of a sexual nature immoral and noxious, labeling them pornographic, and attempting to have them suppressed under obscenity and other laws, with varying degrees of success.

▪Such works have also often been subject to censorship and other legal restraints to publication, display or possession. Such grounds and even the definition of pornography have differed in various historical, cultural, and national contexts.

▪Social attitudes towards the discussion and presentation of sexuality have become more tolerant and legal definitions of obscenity have become more limited, leading to an industry for the production and consumption of pornography in the latter half of the 20th century.

▪The introduction of home video and the Internet saw a boom in the worldwide porn industry that generates billions of dollars annually.

▪Commercialized pornography accounts for over US$2.5 billion in the United States alone, including the production of various media and associated products and services.

6. Intellectual property

Q. What do you mean by Intellectual property? W/13, S/14 CT, W/13, S/14, W/14 , S/15 CSE

Intellectual property (**IP**) is a term referring to creations of the intellect for which a monopoly is assigned to designated owners by law. Some common types of intellectual property rights (IPR) are copyright, patents, and industrial design rights; and the rights that protect trademarks, trade dress, and in some jurisdictions trade secrets: all these cover music, literature, and other artistic works; discoveries and inventions; and words, phrases, symbols, and designs. Intellectual property rights are themselves a form of property, called intangible property.

Intellectual property rights

Intellectual property rights include patents, copyright, industrial design rights, trademarks, plant variety rights, trade dress, and in some jurisdictions trade secrets. There are also more specialized or derived varieties of *sui generis* exclusive rights, such as circuit design rights (called mask work rights in the US) and supplementary protection certificates for pharmaceutical products (after expiry of a patent protecting them) and database rights (in European law).

Patents

A patent is a form of right granted by the government to an inventor, giving the owner the right to exclude others from making, using, selling, offering to sell, and importing an invention for a limited period of time, in exchange for the public disclosure of the invention. An invention is a solution to a specific technological problem, which may be a product or a process and generally has to fulfil three main requirements: it has to be new, not obvious and there needs to be an industrial applicability.

Copyright

A copyright gives the creator of an original work exclusive rights to it, usually for a limited time. Copyright may apply to a wide range of creative, intellectual, or artistic forms, or "works".[Copyright does not cover ideas and information themselves, only the form or manner in which they are expressed.

Industrial design rights

An industrial design right (sometimes called "design right") protects the visual design of objects that are not purely utilitarian. An industrial design consists of the creation of a shape, configuration or composition of pattern or color, or combination of pattern and color in three-dimensional form containing aesthetic value. An industrial design can be a two- or three-dimensional pattern used to produce a product, industrial commodity or handicraft.

Plant varieties

Plant breeders' rights or plant variety rights are the rights to commercially use a new variety of a plant. The variety must amongst others be novel and distinct and for registration the evaluation of propagating material of the variety is examined.

Trademarks

A trademark is a recognizable sign, design or expression which distinguishes products or services of a particular trader from the similar products or services of other traders.

Trade dress

Trade dress is a legal term of art that generally refers to characteristics of the visual appearance of a product or its packaging (or even the design of a building) that signify the source of the product to consumers

Trade secrets

A trade secret is a formula, practice, process, design, instrument, pattern, or compilation of information which is not generally known or reasonably ascertainable, by which a business can obtain an economic advantage over competitors or customers.

6.1 Copyright

Q. What types of work are eligible to be copyright? W/14 CT W/14, IT S/15 CT

▪**Copyright** is a legal right created by the law of a country that grants the creator of an original work exclusive rights to its use and distribution, usually for a limited time.

▪The exclusive rights are not absolute; they are limited by limitations and exceptions to copyright law, including fair use.

▪Copyright is a form of intellectual property, applicable to any expressed representation of a creative work. Under US copyright law, however, legal protection attaches only to *fixed* representations in a tangible medium.

▪ It is often shared among multiple authors, each of whom holds a set of rights to use or license the work, and who are commonly referred to as rights holders. These rights frequently include reproduction, control over derivative works, distribution, public performance, and "moral rights" such as attribution.

▪Copyrights are considered *territorial* rights, which means that they do not extend beyond the territory of a specific jurisdiction. While many aspects of national copyright laws have been standardized through international copyright agreements, copyright laws vary by country.

▪Typically, the *duration* of copyright is the author's life plus 50 to 100 years (that is, copyright typically expires 50 to 100 years after the author dies, depending on the jurisdiction).

▪Some countries require certain copyright formalities to establishing copyright, but most recognize copyright in any completed work, without formal registration. Generally, copyright is enforced as a civil matter, though some jurisdictions do apply criminal sanctions.

▪Most jurisdictions recognize copyright limitations, allowing "fair" exceptions to the creator's exclusivity of copyright and giving users certain rights. The development of digital media and computer network technologies have prompted reinterpretation of these exceptions, introduced new difficulties in enforcing copyright, and inspired additional challenges to copyright law's philosophic basis.

▪Simultaneously, businesses with great economic dependence upon copyright, such as those in the music business, have advocated the extension and expansion of copyright and sought additional legal and technological enforcement.

6.1.1 Copyright Term:

▪Copyright law guarantees developers the rights to their works for a certain amount of time. Since 1960, the term of copyright has been extended 11 times from its original limit of 28 years.
▪The Copyright Term Extension Act, also known as the Sonny Bono Copyright Term Extension Act, signed into law in 1998, established the following time limits:
• For works created after January 1, 1978, copyright protection endures for the life of the author plus 70 years.
• For works created but not published or registered before January 1, 1978, the term endures for the life of the author plus 70 years, but in no case expires earlier than December 31, 2004.

• For works created before 1978 that are still in their original or renewable term of copyright, the total term was extended to 95 years from the date the copyright was originally secured.

▪These extensions were primarily championed by movie studios concerned about retaining rights to their early films.

▪Opponents argued that lengthening the copyright period made it more difficult for artists to build on the work of others, thus stifling creativity and innovation.

6.1.2 Eligible Works:

▪The types of work that can be copyrighted include architecture, art, audiovisual works, choreography, drama, graphics, literature, motion pictures, music, pantomimes, pictures, sculptures, sound recordings, and other intellectual works, as described in Title 17 of the U.S. Code.

▪To be eligible for a copyright, a work must fall within one of the preceding categories, and it must be original.

▪ Copyright law has proven to be extremely flexible in covering new technologies; thus, software, video games, multimedia works, and Web pages can all be protected.

▪However, evaluating the originality of a work is not always a straightforward process, and disagreements over whether or not a work is original sometimes lead to litigation

6.1.3 Fair Use Doctrine

Copyright law tries to strike a balance between protecting an author's rights and enabling public access to copyrighted works. The fair use doctrine was developed over the years as courts worked to maintain that balance. Thefair use doctrineallows portions of copyrighted materials to be used without permission under certain circumstances. Title 17, section 107, of theU.S. Codeestablished four factors that courts should consider when deciding whether a particular use of copyrighted property is fair and can be allowed without penalty:

• The purpose and character of the use (such as commercial use or nonprofit, educational purposes)

• The nature of the copyrighted work

• The portion of the copyrighted work used in relation to the work as a whole

• The effect of the use on the value of the copyrighted work

6.1.4 Software Copyright Protection:

▪The use of copyrights to protect computer software raises many complicated issues of interpretation. For example, a software manufacturer can observe the operation of a competitor's copyrighted program and then create a program that accomplishes the same result and performs in the same manner.

▪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.

▪However, if the new software's manufacturer can establish that it developed the program on its own, without any knowledge of the existing program, there is no infringement.

▪For example, two software manufacturers could conceivably develop separate programs for a simple game such as tic-tac-toe without infringing the other's copyright.

▪An area that holds the potential for software copyright infringement involves the sale of refurbished consumer computer supplies, such as toner and inkjet cartridges.

▪One company that objected to the use of refurbished cartridges was Lexmark International, a manufacturer and supplier of printers and associated supplies. In 2002, Lexmark filed suit against Static Control Components (SCC), a producer of components used to make refurbished printer cartridges.

▪ The suit alleged that SCC's Smartek chips included Lexmark software in violation of copyright law. (The software is necessary to allow the refurbished toner cartridges to work with Lexmark's printers.)

6.2 Digital Millennium Copyright Act

▪The **Digital Millennium Copyright Act** (**DMCA**) is a United States copyright law that implements two 1996 treaties of the World Intellectual Property Organization (WIPO).

▪ It criminalizes production and dissemination of technology, devices, or services intended to circumvent measures (commonly known as digital rights management or DRM) that control access to copyrighted works.

▪ It also criminalizes the act of circumventing an access control, whether or not there is actual infringement of copyright itself.

▪In addition, the DMCA heightens the penalties for copyright infringement on the Internet. Passed on October 12, 1998, by a unanimous vote in the United States Senate and signed into law by President Bill Clinton on October 28, 1998, the DMCA amended Title 17 of the United States Code to extend the reach of copyright, while limiting the liability of the providers of online services for copyright infringement by their users.

▪The DMCA's principal innovation in the field of copyright is the exemption from direct and indirect liability of Internet service providers and other intermediaries.

▪This exemption was adopted by the European Union in the Electronic Commerce Directive 2000. The Copyright Directive 2001 implemented the 1996 WIPO Copyright Treaty in the EU.

Provisions

6.2.1 Title I: WIPO Copyright and Performances and Phonograms Treaties Implemention Act

DMCA Title I, the WIPO Copyright and Performances and Phonograms Treaties Implementation Act, amends U.S. copyright law to comply with the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty, adopted at the WIPO Diplomatic Conference in December 1996. The treaties have two major portions. One portion includes works covered by several treaties in U.S. copy prevention laws and gave the title its name. For further analysis of this portion of the Act and of cases under it, see WIPO Copyright and Performances and Phonograms Treaties Implementation Act.

The second portion (17 U.S.C. 1201) is often known as the DMCA anti-circumvention provisions. These provisions changed the remedies for the circumvention of copy-prevention systems (also called "technical protection measures") and required that all analog video recorders have support for a specific form of copy prevention created by Macrovision (now Rovi Corporation) built in, giving Macrovision an effective monopoly on the analog video-recording copy-prevention market. The section contains a number of specific limitations and exemptions, for such things as government research and reverse engineering in specified situations. Although, section 1201(c) of the title stated that the section does not change the underlying substantive copyright infringement rights, remedies, or defenses, it did not make those defenses available in circumvention actions. The section does not include a fair use exemption from criminality nor a scienter requirement, so criminal liability could attach even unintended circumvention for legitimate purposes.[3] The Unlocking Technology Act of 2013 was introduced to attempt to fix these oversights, which include prohibitions on unlocking one's own cell phone.[4][5]However, no action was taken by Congress as of the end of 2013.

6.2.2 Title II: Online Copyright Infringement Liability Limitation Act

DMCA Title II, the Online Copyright Infringement Liability Limitation Act ("OCILLA"), creates a safe harbor for online service providers (OSPs, including ISPs) against copyright infringement liability, provided they meet specific requirements. OSPs must adhere to and qualify for certain prescribed

safe harbor guidelines and promptly block access to alleged infringing material (or remove such material from their systems) when they receive notification of an infringement claim from a copyright holder or the copyright holder's agent. OCILLA also includes a counter notification provision that offers OSPs a safe harbor from liability to their users when users claim that the material in question is not, in fact, infringing. OCILLA also facilitates issuing of subpoenas against OSPs to provide their users' identity.

6.2.3 Title III: Computer Maintenance Competition Assurance Act

DMCA Title III modified of the copyright title so that those repairing computers could make certain temporary, limited copies while working on a computer

6.2.4 Title IV: Miscellaneous Provisions

DMCA Title IV contains an assortment of provisions:

- Clarified and added to the duties of the Copyright Office.
- Added ephemeral copy for broadcasters provisions, including certain statutory licenses.
- Added provisions to facilitate distance education.
- Added provisions to assist libraries with keeping phonorecords of sound recordings.
- Added provisions relating to collective bargaining and the transfer of movie rights.

6.2.5 Title V: Vessel Hull Design Protection Act

DMCA Title V added sections 1301 through 1332 to add a *sui generis* protection for boat hull designs. Boat hull designs were not considered covered under copyright law because they are useful articles whose form cannot be cleanly separated from their function

6.3 Patent

Q. Explain Patents W/14 IT, S/15 CT

▪A **patent** (is a set of exclusive rights granted by as overeign state to an inventor or assignee for a limited period of time in exchange for detailed public disclosure of an invention.

▪An invention is a solution to a specific technological problem and is a product or a process. Patents are a form of intellectual property.

▪The procedure for granting patents, requirements placed on the patentee, and the extent of the exclusive rights vary widely between countries according to national laws and international agreements.

▪Typically, however, a granted patent application must include one or more claims that define the invention.

▪ A patent may include many claims, each of which defines a specific property right. These claims must meet relevant patentability requirements, such as novelty, usefulness, and non-obviousness.
▪The exclusive right granted to a patentee in most countries is the right to prevent others, or at least to try to prevent others, from commercially making, using, selling, importing, or distributing a patented invention without permission.

▪Under the World Trade Organization's (WTO) Agreement on Trade-Related Aspects of Intellectual Property Rights, patents should be available in WTO member states for any invention, in all fields of technology, and the term of protection available should be a minimum of twenty years.

▪Nevertheless, there are variations on what is patentable subject matter from country to country.

Definition

▪The word patent means "to lay open" (i.e., to make available for public inspection). More directly, it is a shortened version of the term letters patent, which was a royal decree granting exclusive rights to a person, predating the modern patent system. Similar grants included and patents, which were land grants by early state governments in the USA, and printing patents, a precursor of modern copyright.

▪In modern usage, the term patent usually refers to the right granted to anyone who invents any new, useful, and non-obvious process, machine, article of manufacture, or composition of matter. ▪Some other types of intellectual property rights are also called patents in some jurisdictions: industrial design rights are called design patents in the US plant breeders' rights are sometimes called plant patents, and utility models and Gebrauchsmuster are sometimes called petty patents or innovation patents.

▪The additional qualification utility patent is sometimes used (primarily in the US) to distinguish the primary meaning from these other types of patents. Particular species of patents for inventions include biological patents, business method patents, chemical patents and software patents.

6.3.1 Software patent

▪**software patent** has been proposed by the Foundation for a Free Information Infrastructure (FFII) as being a "patent on any performance of a computer realised by means of a computer program". There is no legal or conclusive definition for a software patent.

▪Globally the situation is more complex and reflects varying cultural views of invention itself. Most countries place some limits on the patenting of inventions involving software, but there is no one legal definition of a software patent.

▪For example, U.S. patent law excludes "abstract ideas", and this has been used to refuse some patents involving software. In Europe, "computer programs as such" are excluded from patentability, thus European Patent Office policy is consequently that a program for a computer is not patentable if it does not have the potential to cause a "further technical effect" beyond the inherent technical interactions between hardware and software.

There is a debate over the extent to which software patents should be granted, if at all. Important issues concerning software patents include:

- Whether software patents should be allowed, and if so, where the boundary betweenpatentable and non-patentable software should lie;
- Whether the inventive step and non-obviousness requirement is applied too loosely to software; and
- Whether patents covering software discourage, rather than encourage, innovation

6.4 Software Cross-Licensing Agreements:

Q. Explain Cross-Licensing Agreements W/13, W/14 CT S/15 CT

A **cross-licensing** agreement is a contract between two or more parties where each party grants rights to their intellectual property to the other parties.

6.4.1 Patent law

▪In patent law, a **cross-licensing agreement** is an agreement according to which two or more parties grant a license to each other for the exploitation of the subject-matter claimed in one or more of the patents each owns.

▪ Usually, this type of agreement happens between two parties in order to avoid litigation or to settle an infringement dispute. Very often, the patents that each party owns covers different essential aspects of a given commercial product.

▪ Thus by cross licensing, each party maintains their freedom to bring the commercial product to market. The term "cross licensing" implies that neither party pays monetary royalties to the other party, although this may be the case.

▪For example, Microsoft and JVC entered into a cross license agreement in January 2008. Each party, therefore, is able to practice the inventions covered by the patents included in the agreement. This benefits competition by allowing each more freedom to design products covered by the others patents without provoking a patent infringement lawsuit.

▪Parties that enter into cross-licensing agreements must be careful not to violate antitrust laws and regulations. This can easily become a complex issue, involving (as far as the European Union is concerned)

▪One of the limitations of cross licensing is that it is ineffective against patent holding companies. The primary business of a patent holding company is to license patents in exchange for a monetary royalty. Thus, they have no need for rights to practice other companies' patents. These companies are often referred to pejoratively as patent trolls.

The economics literature has shown that firms with high capital intensities are more likely to strike a cross-licensing deal.

6.4.2 Non patent law

Other non-patent intellectual property such as copyright and trademark can also be cross-licensed. For example, a literary work and an anthology that includes that literary work may be cross-licensed between two publishers. A cross-license for computer software may involve a combination of patent, copyright, and trademark licensing.

DEFENSIVE PUBLISHING AND PATENT TROLLS

Patenting is extremely expensive and most companies have more innovative ideas than budgeted patent resources. Who can afford to patent everything? On the other hand, who can afford to let competitors patent technology used in your products and services? Worse yet, how do you know, years in advance, which patentable ideas you will need for your products and services? **Defensive publishing is a low cost way to prevent competitors from obtaining patents and protect your freedom to practice.**

Patent trolls are individuals or investment funds that purchase patents as a long-term investment, seeking the income stream from collecting royalties. The term has a perjorative connotation, casting these patent holders in a different light from companies that actually manufacture products or deliver services based on the patents. Patent trolls are frequently engaged in litigation against patent infringers who attempt to use the patented knowledge without paying for it (and who show their resentment at being forced to pay by characterizing their pursuers as “trolls”).

Examples:

Patent trolls tend to be long-term investors who seek ongoing royalty income from portfolios of patents, analogous to investors who collect interest income from bond portfolios.

SUBMARINE PATENTS AND PATENTS FARMING

A SubmarinePatent is a patent which an "inventor" files on a device or technology that doesn't exist yet, or which has not yet been successfully implemented. Using various procedural mechanisms, the filer *intentionally* delays issue of the patent, sometimes for years, until a practical implementation of the device/technology appears on the market. At that time, the filer allows the patent to "come to the surface" and demands royalties from the party who did the real work.

For example, under the old system, someone in 1950 could have filed a patent on, say, a packet-based computer network router, though there were as yet hardly any computers to speak of. By requesting repeated "continuations" during the patent application process, the filer could force the patent to be delayed indefinitely until packet-based routers started to come onto the market, say in 1970. The filer then stops requesting continuations, the patent issues, and the patent-seeker can collect royalties on network routers for 17 years from that point, until 1987.

Patent Farming a strategy that a devious patent holder might influence a standards organization to make use of its patented item without revealing the existence of the patent. Later, the patent holder might demand royalties from all parties that use the standard.

6.5 Trade secret

Q. Explain **Trade Secret** S/15 CT

A **trade secret** is a formula, practice, process, design, instrument, pattern, commercial method, or compilation of information which is not generally known or reasonably ascertainable by others, and by which a business can obtain an economic advantage over competitors or customers.[1] In some jurisdictions, such secrets are referred to as "confidential information", but are generally not referred to as "classified information" in the United States, since that refers to government secrets protected by a different set of laws and practices.

Definition

The precise language by which a trade secret is defined varies by jurisdiction (as do the particular types of information that are subject to trade secret protection). However, there are three factors that, although subject to differing interpretations, are common to all such definitions: a trade secret is information that:

- Is not generally known to the public;
- Confers some sort of economic benefit on its holder (where this benefit must derive *specifically* from its not being publicly known, not just from the value of the information itself);
- Is the subject of reasonable efforts to maintain its secrecy.

6.5.1 Trade Secret Laws

‣Trade secret protection laws vary greatly from country to country.

‣For example, the Philippines provides no legal protection for trade secrets. In some European countries, pharmaceuticals, methods of medical diagnosis and treatment, and information technology cannot be patented.

‣Many Asian countries require foreign corporations operating there to transfer rights to their technology to locally controlled enterprises.

6.5.2 Uniform Trade Secrets Act (UTSA)

The Uniform Trade Secrets Act (UTSA) was drafted in the 1970s to bring uniformity to all states in the area of trade secret law. The first state to enact the UTSA was Minnesota in 1981, followed by

39 more states and the District of Columbia. The UTSA defines a trade secret as“I nformation, including a formula, pattern, compilation, program, device, method, technique, or process, that:

• Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by, persons who can obtain economic value from its disclosure or use

• Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy” Under these terms, computer hardware and software can qualify for trade secret protection by the UTSA

6.5.3 The Economic Espionage Act (EEA) (1996):

‣The Economic Espionage Act (EEA) of 1996 imposes penalties of up to $10 million and 15 years in prison for the theft of trade secrets.

‣Before the EEA, there was no specific criminal statute to help pursue economic espionage; the FBI was investigating nearly 800 such cases in 23 countries when the EEA was enacted.

‣Today, intellectual property loss from industrial and economic espionage costs U.S.-based businesses more than $300 billion annually, according to estimates by Guardsmark, a New York security services firm. As with the UTSA, information is considered a trade secret under the EEA only if companies take steps to protect it.

6.6 KEY INTELLECTUAL PROPERTY ISSUES:

Q. What are different key issue that apply to intellectual property and information? W/14 IT

Q. What is open source code? W/14 IT

‣several issues that apply to intellectual property and information technology, including plagiarism, reverse engineering, open source code, competitive intelligence, and cyber squatting.

6.6.1 Plagiarism:

Q. Short note on Plagiarism W/13 IT

‣Plagiarism is the act of stealing someone’s ideas or words and passing them off as one’s own. The explosion of electronic content and the growth of the Web have made it easy to cut and paste paragraphs into term papers and other documents without proper citation or quotation marks.

‣To compound the problem, hundreds of online“ paper mills” enable users to download entire term papers. Although so me sites post warnings that their services should be used for research purposes only, many users pay scant heed.

‣ As a result, plagiarism has become an issue from elementary schools to the highest levels of academia.

6.6.2 Reverse engineering

Q. Short note on Reverse engineering W/13 IT, S/15 CT S/15 CSE

‣**Reverse engineering**, also called **back engineering**, is the processes of extracting knowledge or design information from anything man-made and re-producing it or reproducing anything based on the extracted information.

‣The process often involves disassembling something (a mechanical device, electronic component, computer program, or biological, chemical, or organic matter) and analyzing its components and workings in detail.

‣The reasons and goals for obtaining such information vary widely from everyday or socially beneficial actions, to criminal actions, depending upon the situation. Often no intellectual property rights are breached, such as when a person or business cannot recollect how something was done, or what something does, and needs to reverse engineer it to work it out for themselves.

‣Reverse engineering is also beneficial in crime prevention, where suspected malware is reverse engineered to understand what it does, and how to detect and remove it, and to allow computers and devices to work together ("interoperate") and to allow saved files on obsolete systems to be used in newer systems.

‣By contrast, reverse engineering can also be used to "crack" software and media to remove their copy protection or to create a (possibly improved) copyor even a knockoff; this is usually the goal of a competitor.

‣Reverse engineering has its origins in the analysis of hardware for commercial or military advantage.

‣ However, the reverse engineering process in itself is not concerned with creating a copy or changing the artifact in some way; it is only ananalysis in order to deduce design features from products with little or no additional knowledge about the procedures involved in their original production.

‣ In some cases, the goal of the reverse engineering process can simply be are documentation of legacy systems. Even when the product reverse engineered is that of a competitor, the goal may not be to copy them, but to perform competitor analysis.

‣ Reverse engineering may also be used to create interoperable products; despite some narrowly tailored US and EU legislation, the legality of using specific reverse engineering techniques for this purpose has been hotly contested in courts worldwide for more than two decades.[

6.6.3 Open source code

‣In production and development, **open source** as a development model promotes a universal access via a free license to a product's design or blueprint, and universal redistribution of that design or blueprint, including subsequent improvements to it by anyone.

‣ Before the phrase *open source* became widely adopted, developers and producers used a variety of other terms. *Open source* gained hold with the rise of the Internet, and the attendant need for massive retooling of the computing source.

‣Opening the source code enabled a self-enhancing diversity of production models, communication paths, and interactive communities.

‣The open-source software movement arose to clarify the environment that the new copyright,licensing, domain, and consumer issues created

‣Generally, open source refers to a computer program in which the source code is available to the general public for use and/or modification from its original design. Open-source code is meant to be a collaborative effort, where programmers improve upon the source code and share the changes within the community.

‣Typically this is not the case, and code is merely released to the public under some license. Others can then download, modify, and publish their version (fork) back to the community. Today you find more projects with forked versions than unified projects worked by large teams.

‣Many large formal institutions have sprung up to support the development of the open source movement, including the Apache Software Foundation, which supports projects such as the open source framework behind big data Apache Hadoop and an open-source HTTP server Apache HTTP.

‣The open-source model is based on a more decentralized model of production, in contrast with more centralized models of development such as those typically used in commercial software companies.

‣A main principle of open-source software development is peer production, with products such as source code, "blueprints", and documentation available to the public at no cost.

‣The open source movement in software began as a response to the limitations of proprietary code, and has since spread across different fields.

‣This model is also used for the development of open-source-appropriate technologies, solar photovoltaic technology[6] and open-source drug discovery.

6.6.4 Competitive intelligence

‣**Competitive intelligence** is the action of defining, gathering, analyzing, and distributing intelligence about products, customers, competitors, and any aspect of the environment needed to support executives and managers making strategic decisions for an organization.

‣Competitive intelligence essentially means understanding and learning what's happening in the world outside your business so one can be as competitive as possible.

‣It means learning as much as possible—as soon as possible—about one's industry in general, one's competitors, or even one's county's particular zoning rules. In short, it empowers you to anticipate and face challenges head on.

Key points of this definition:

1. Competitive intelligence is an ethical and legal business practice, as opposed to industrial espionage, which is illegal.
2. The focus is on the external business environment
3. There is a process involved in gathering information, converting it into intelligence and then utilizing this in business decision making. Some CI professionals erroneously emphasize that if the intelligence gathered is not usable, or actionable, then it is not intelligence.

‣A more focused definition of CI regards it as the organizational function responsible for the early identification of risks and opportunities in the market before they become *obvious*.

‣ Experts also call this process the early signal analysis. This definition focuses attention on the difference between dissemination of widely available factual information (such as market statistics, financial reports, newspaper clippings) performed by functions such as libraries and information centers, and competitive intelligence which is a *perspective* on developments and events aimed at yielding a competitive edge.

‣The term CI is often viewed as synonymous with competitor analysis, but competitive intelligence is more than analyzing competitors—it is about making the organization more competitive relative to its

entire environment and stakeholders: customers, competitors, distributors, technologies, and macroeconomic data.

6.6.5 Industrial espionage

‣**Industrial espionage**, **economic espionage** or **corporate espionage** is a form of espionage conducted for commercial purposes instead of purely national security.

‣ Economic espionage is conducted or orchestrated by governments and is international in scope, while industrial or corporate espionage is more often national and occurs between companies or corporations

Competitive intelligence and economic or industrial espionage

Q. Difference between Competitive intelligence and industrial espionage W/13 CSE S/15 CT S/15 CSE

‣"Competitive intelligence" levels out two scenarios of description as the legal and ethical activity of systematically gathering, analyzing and managing information on industrial competitors becomes beneficial.

‣ It may include activities such as examining newspaper articles, corporate publications, websites, patent filings, specialised databases, information at trade shows and the like to determine information on a corporation.

‣ The compilation of these crucial elements is sometimes termed CIS or CRS, a Competitive Intelligence Solution or Competitive Response Solution.

‣With its roots in market research, "competitive intelligence" has been described as the "application of principles and practices from military and national intelligence to the domain of global business";

‣ it is the business equivalent of open-source intelligence.

‣The difference between competitive intelligence and economic or industrial espionage is not clear; one needs to understand the legal basics to recognize how to draw the line between the two.

‣ Others maintain it is sometimes quite difficult to tell the difference between legal and illegal methods, especially if considering the ethical side of information gathering, making the definition even more elusive.

6.6.6 Cyber squatting

Q.What is Cyber squatting and what strategy should be used to protect an oragnization? S/14 , S/15 CSE

‣**Cyber squatting** (also known as **domain squatting**), according to the United States federal law known as the Anticybersquatting Consumer Protection Act, is registering, trafficking in, or using an Internet domain name with bad faithintent to profit from the goodwill of a trademark belonging to someone else.

‣The cybersquatter then offers to sell the domain to the person or company who owns a trademark contained within the name at an inflated price.

‣The term is derived from "squatting", which is the act of occupying an abandoned or unoccupied space or building that the squatter does not own, rent, or otherwise have permission to use.

6.6.7 Cyber bullying

‣**Cyberbullying** is the use of social networks to repeatedly harm or harass other people in a deliberate manner.

‣According to U.S. Legal Definitions, "cyber-bullying could be limited to posting rumors or gossips about a person in the internet bringing about hatred in other's minds; or it may go to the extent of personally identifying victims and publishing materials severely defaming and humiliating them".

Distinctions

Legal definition

Cyberbullying is defined in legal glossaries as

- actions that use information and communication technologies to support deliberate, repeated, and hostile behavior by an individual or group, that is intended to harm another or others.
- use of communication technologies for the intention of harming another person
- use of internet service and mobile technologies such as web pages and discussion groups as well as instant messaging or SMS text messaging with the intention of harming another person.

Examples of what constitutes cyberbullying include communications that seek to intimidate, control, manipulate, put down,falsely discredit, or humiliate the recipient.

‣The actions are deliberate, repeated, and hostile behavior intended to harm another. Cyberbullying has been defined by The National Crime Prevention Council: "When the Internet, cell phones or other devices are used to send or post text or images intended to hurt or embarrass another person

‣A cyberbully may be a person whom the target knows or an online stranger.

‣A cyberbully may be anonymous and may solicit involvement of other people online who do not even know the target.

‣This is known as a "digital pile-on. Cyber bullying has been defined as "when the Internet, cell phones or other devices are used to send or post text or images intended to hurt or embarrass another person".[8] Other researchers use similar language to describe the phenomenon.

6.6.8 Cyberbullying vs. cyberstalking

‣The practice of cyber bullying is not limited to children and, while the behavior is identified by the same definition when practiced by adults, the distinction in age groups sometimes refers to the abuse as cyber stalking or cyber harassment when perpetrated by adults toward adults. ‣Common tactics used by cyber stalkers are performed in public forums, social media or online information sites and are intended to threaten a victim's earnings, employment, reputation, or safety.

‣Behaviors may include encouraging others to harass the victim and trying to affect a victim's online participation.

‣Many cyber stalkers try to damage the reputation of their victim and turn other people against them.

‣Cyber stalking may include false accusations, monitoring, making threats, identity theft, damage to data or equipment, the solicitation of minors for sex, or gathering information in order to harass.

‣A repeated pattern of such actions and harassment against a target by an adult constitutes cyber stalking.

‣Cyber stalking often features linked patterns of online and offline behavior.

‣There are consequences of law in offline stalking and online stalking, and cyber stalkers can be put in jail Cyber stalking is a form of cyber bullying.

6.6.9 Traditional bullying

‣Certain characteristics inherent in online technologies increase the likelihood that they will be exploited for deviant purposes.

‣ Unlike physical bullying, electronic bullies can remain virtually anonymous using temporary email accounts, pseudonyms in chat rooms, instant messaging programs, cell-phone text messaging, and other Internet venues to mask their identity; this perhaps frees them from normative and social constraints on their behavior.

‣Additionally, electronic forums often lack supervision. While chat hosts regularly observe the dialog in some chat rooms in an effort to police conversations and evict offensive individuals, personal messages sent between users (such as electronic mail or text messages) are viewable only by the sender and the recipient, thereby falling outside the regulatory reach of such authorities.

‣ In addition, when teenagers know more about computers and cellular phones than their parents or guardians, they are therefore able to operate the technologies without concern that a parent will discover their experience with bullying (whether as a victim or offender).

‣Another factor is the inseparability of a cellular phone from its owner, making that person a perpetual target for victimization. Users often need to keep their phone turned on for legitimate purposes, which provides the opportunity for those with malicious intentions to engage in persistent unwelcome behavior such as harassing telephone calls or threatening and insulting statements via the cellular phone’s text messaging capabilities.

‣Cyber bullying thus penetrates the walls of a home, traditionally a place where victims could seek refuge from other forms of bullying. Compounding this infiltration into the home life of the cyberbully victim is the unique way in which the internet can "create simultaneous sensations of exposure (the whole world is watching) and alienation (no one understands)."

‣One possible advantage for victims of cyberbullying over traditional bullying is that they may sometimes be able to avoid it simply by avoiding the site/chat room in question.

‣ Email addresses and phone numbers can be changed; in addition, most email accounts now offer services that will automatically filter out messages from certain senders before they even reach the inbox, and phones offer similar caller ID functions.

‣However, this does not protect against all forms of cyber bullying. Publishing of defamatory material about a person on the internet is extremely difficult to prevent and once it is posted, many people or archiving services can potentially download and copy it, at which point it is almost impossible to remove from the Internet. Some perpetrators may post victims' photos, or victims' edited photos featuring defaming captions or pasting victims' faces on nude bodies.

‣Cyber bullying is sometimes used by the targets of bullying to retaliate against their bullies, since factors such as anonymity, absence of the bully's supporting friends, and irrelevancy of physical strength in the online environment, make it safer to counterattack the bully by that means.

6.6.10 In social media

‣Cyberbullying can take place on social media sites such as Facebook, Myspace, and Twitter. "By 2008, 93% of young people between the ages of 12 and 17 were online.

‣In fact, youth spend more time with media than any single other activity besides sleeping." There are many risks attached to social media sites, and cyberbullying is one of the larger risks.
‣One million children were harassed, threatened or subjected to other forms of cyberbullying on Facebook during the past year, while 90 percent of social-media-using teens who have witnessed online cruelty say they have ignored mean behavior on social media, and 35 percent have done this frequently.

‣95 percent of social-media-using teens who have witnessed cruel behavior on social networking sites say they have seen others ignoring the mean behavior, and 55 percent witness this frequently.

‣The most recent case of cyber-bullying and illegal activity on Facebook involved a memorial page for the young boys who lost their lives to suicide due to anti-gay bullying.

‣The page quickly turned into a virtual grave desecration and platform condoning gay teen suicide and the murdering of homosexuals.

‣ Photos were posted of executed homosexuals, desecrated photos of the boys who died and supposed snuff photos of gays who have been murdered. Along with this were thousands of comments encouraging murder sprees against gays, encouragement of gay teen suicide, death threats etc. In addition, the page continually exhibited pornography to minors

Q. What Are The Standards That The Warranty Of Merchantability **Requires To Meet? W14 CT**

▪The **warranty of merchantability** is implied, unless expressly disclaimed by name, or the sale is identified with the phrase "as is" or "with all faults."

▪ To be "merchantable", the goods must reasonably conform to an ordinary buyer's expectations, i.e., they are what they say they are.

▪ For example, a fruit that looks and smells good but has hidden defects would violate the implied warranty of merchantability if its quality does not meet the standards for such fruit "as passes ordinarily in the trade".

▪In Massachusetts consumer protectionlaw, it is illegal to disclaim this warranty on household goods sold to consumers etc.

▪The **warranty of fitness for a particular purpose** is implied when a buyer relies upon the seller to select the goods to fit a specific request.

▪For example, this warranty is violated when a buyer asks a mechanic to provide snow tires and receives tires that are unsafe to use in snow.

▪This implied warranty can also be expressly disclaimed by name, thereby shifting the risk of unfitness back to the buyer.

▪Another implied warranty is the **warranty of title**, which implies that the seller of goods has the right to sell them (e.g., they are not stolen, or patent infringements, or already sold to someone else).

▪This theoretically saves a buyer from having to "pay twice" for a product, if it is confiscated by the rightful owner, but only if the seller can be found and makes restitution.

Merchantability

▪An **implied warranty of merchantability** is a warranty implied by law that goods are reasonably fit for the general purpose for which they are sold.

International sales law

▪In international sales law, merchantability forms part of the ordinary purpose of the goods. According to Article 35(2)(a) of the United Nations Convention on Contracts for the International Sale of Goods, a seller must provide goods fit for their ordinary purpose.

United States

In the United States, the obligation is in Article 2 of the Uniform Commercial Code (UCC). This warranty will apply to a merchant (that is, a person who makes an occupation of selling things) who regularly deals in the type of merchandise sold.

Under US law, goods are 'merchantable' if they meet the following conditions:

1. The goods must conform to the standards of the trade as applicable to the contract for sale.
2. They must be fit for the purposes such goods are ordinarily used, even if the buyer ordered them for use otherwise.
3. They must be uniform as to quality and quantity, within tolerances of the contract for sale.
4. They must be packed and labeled per the contract for sale.
5. They must meet the specifications on the package labels, even if not so specified by the contract for sale.

If the merchandise is sold with an express "guarantee", the terms of the implied warranty of merchantability will fill the gaps left by that guarantee. If the terms of the express guarantee are not specified, they will be considered to be the terms of the implied warranty of merchantability. The UCC allows sellers to disclaim the implied warranty of merchantability, provided the disclaimer is made conspicuously and the disclaimer explicitly uses the term "merchantability" in the disclaimer.[1] Some states, however, have implemented the UCC such that this can not be disclaimed.

Habitability

▪An implied warranty of habitability, generally, is a warranty implied by law that by leasing or buying a residential property, the leasor or seller is promising that the property is suitable to be lived in.

▪The warranty of habitability can be breached if there is no heat, hot water, or other essential services. Also, safety issues like no smoke alarm or other fire code issues can be considered to make a dwelling uninhabitable. Also, if the municipality has not issued a certificate of occupancy, it is not legal and is thus uninhabitable.

▪The breach of the implied warrant of habitability can be used to legally break a lease.

▪If the factors have been created or are controllable by the landlord and he or she has not fixed them despite ample written notification, this situation can also be considered constructive eviction, which allows the tenant to break the lease, but also may allow the tenant to sue for damages in some jurisdictions.

Chapter 7
Computer forensics

▪**Computer forensics** (sometimes known as **computer forensic science** is a branch of digital forensic science pertaining to illegal evidence found in computers and digital storage media.

▪The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information.

▪Although it is most often associated with the investigation of a wide variety of computer crime, computer forensics may also be used in civil proceedings.

▪The discipline involves similar techniques and principles to data recovery, but with additional guidelines and practices designed to create a legal audit trail.

▪Evidence from computer forensics investigations is usually subjected to the same guidelines and practices of other digital evidence.

▪ It has been used in a number of high-profile cases and is becoming widely accepted as reliable within U.S. and European court systems.

Use as evidence

▪In court, computer forensic evidence is subject to the usual requirements for digital evidence. This requires that information be authentic, reliably obtained, and admissible.

▪ Different countries have specific guidelines and practices for evidence recovery.

▪In the United Kingdom, examiners often follow Association of Chief Police Officers guidelines that help ensure the authenticity and integrity of evidence. While voluntary, the guidelines are widely accepted in British courts.

Q.4 B

1. Shred All Identifying Documents, Bank Slips, Etc.

Bank deposit receipts, credit card statements, old documents, anything with sensitive information should be properly disposed of. If you don't have a fireplace, consider investing in a low-cost paper shredder. Identity thieves can learn a lot from rifling through trash -- don't let yours give away your identity.

2. Shop Online Only on Secure Web Sites

Shopping online is safe -- when you use secure web pages. Check the bottom of your browser and look for a locked graphic, or look for "https" in the address bar. This means you are on a secure web page and your data is encrypted. Without a secure connection, hackers can eavesdrop on your transaction and grab your private data.

3. Don't Fall for Phishing Scams

Phishing is a technique employed by identity thieves through email or online chat services. The thief pretends to represent a company, such as PayPal or your credit card issuer, and informs you that you need to respond with some information or click on a link. The thief may even claim to represent a charity or sweepstakes giveaway. Don't fall for it. Don't respond and don't click the link, even if it *appears* to be a legitimate link. Responsible organizations will not contact you in this way.

4. Beware of Telephone Scams

Never give out personal information over the phone to someone who calls you claiming to represent a bank, credit card company, charity, or other organization. People are not always who they claim to be. You could be talking to a scam artist who is sweet-talking you out of your credit card or bank account number. This is an old scam, but still widely practiced today because it works. Don't let it work on you.

5. Keep Anti-Virus and Anti-Spyware Software Up to Date

A computer virus or trojan horse spyware program that sneaks its way onto your computer can compromise your private information. These malicious programs can scan through your entire hard drive and send what it finds out over the internet. To combat this threat, be sure to run an anti-virus program and at least one anti-spyware program,

6. Check Your Credit Report

. Verify that the information is correct and check for suspicious activity, particularly mysterious new accounts opened. For even better protection, sign up for a service that notifies you when changes occur to your credit report.

7. Ask About Identity Theft Prevention Procedures

Ask your bank about what they are doing to combat identity theft. Call your credit card company and find out if you will be liable for fraudulent charges. Ask your employer about what steps are taken to safeguard sensitive employee data. It's your data; you should know how it is managed.

8. Secure Your Important Documents

Your social security card, passport, birth certificate and other identifying materials are highly sought-after by identity thieves and can command top dollar on the black market. Be sure that your documents are safely stored, preferably in a locked box tucked away and out of sight. Do not regularly carry these documents on you. When you travel, pay special attention to securing your passport. Leave it in a hotel room safe at all times.

9. Be Vigilant About Your Social Security Number

Some institutions--insurers, colleges, etc.--prefer to use your social security number as their identification number for you. This is very foolish, as it essentially deprivatizes this number. Because your social security number can be used to gain access to a lot of other private information about you, opt out of allowing institutions to use it. Another number can be substituted instead.

10. Be Careful With Your Mail

Of course tampering with someone's mail is a federal offense, but that doesn't stop people from doing it. Try not to let incoming mail sit in your mailbox for a long time. If you are going to be away, have the post office hold your mail for you. When sending out sensitive mail, consider dropping it off at a secure collection box or at the post office itself.

8

THE IMPACT OF INFORMATION TECHNOLOGY ON PRODUCTIVITY AND QUALITY OF LIFE

8. THE IMPACT OF IT ON THE STANDARD OF LIVING AND WORKER PRODUCTIVITY:

Q. Define Productivity and discuss the relationship between IT investment and Productivity growth S/14 CT S/15 CT
Q. What impact has IT had on the standard of living and worker productivity? W/13 S/14 W/14 CSE S/14 S/15 IT

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.

8.1 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.

‣ For example, productivity in a factory might be measured by the number of labor hours it takes to produce one item, while productivity in a service sector company might be measured by the annual revenue an employee generates divided by the employee's annual salary.

‣ Most countries have continually been able to produce more goods and services over time—not through a proportional increase in input but by making production more efficient.

‣These gains in productivity have led to increases in the GDP-based standard of living because the average hour of labor produced more goods and services. The Bureau of Labor Statistics tracks U.S. productivity on a quarterly basis.

‣In the United States, labor productivity growth has averaged about 2 percent per year for the past century, meaning that living standards have doubled about every 36 years.

‣ Innovation is a key factor in productivity improvement, and IT has played an important role in enabling innovation. Progressive management teams use IT, as well as other new technology and capital investment, to implement innovations in products, processes, and services.

‣In the early days of IT in the 1960s, productivity improvements were easy to measure.

‣For example, midsized companies often had a dozen or more accountants focused solely on payroll-related accounting. When businesses learned to apply automated payroll systems, fewer accounting employees were needed. The productivity gains from such IT investments were obvious.

‣Today, organizations are trying to further improve IT systems and business processes that have already gone through several rounds of improvement.

‣Organizations are also adding new IT capabilities to help workers who already have an assortment of personal productivity applications on their desktop computers, laptops, and personal digital assistants (PDAs).

‣ Instead of eliminating workers, companies are saving workers small amounts of time each day. Whether these saved minutes actually result in improved worker productivity is a matter for debate.

‣Many analysts argue that workers merely use the extra time to do some small task they didn't have time to do before, such as respond to e-mail they would have ignored. These minor gains make it harder to quantify the benefits of today's IT investments on worker productivity.

8.2 Telework:

Q. Define the Telework and identify several factors that have increased the level of telework. W/14 S/15 CT
Q. Pros and cons of Telework W/13 IT

‣**Telecommuting**, **remote work**, or **telework** is a work arrangement in which employees do not commute to a central place of work. A person who telecommutes is known as a "telecommuter", "teleworker", and sometimes as a "home-sourced," or "work-at-home" employee.

‣Many telecommuters work from home, while others, sometimes called "nomad workers", use mobile telecommunications technology to work from coffee shops or other locations.

Definition

‣Although the concepts of "telecommuting" and "telework" are closely related, there is still a difference between the two.

‣All types of technology-assisted work conducted outside of a centrally located work space (including work undertaken in the home, outside calls, etc.) are regarded as telework.

‣Telecommuters often maintain a traditional office and usually work from an alternative work site around 1 to 3 days a week. Telecommuting refers more specifically to work undertaken at a location that reduces commuting time.

‣ These locations can be inside the home or at some other remote workplace, which is facilitated through a broadband connection, computer or phone lines, or any other electronic media used to interact and communicate.

‣As a broader concept than telecommuting, telework has four dimensions in its definitional framework: work location, that can be anywhere outside of a centralized organizational work place; usage of ICTs (information and communication technologies) as technical support for telework; time distribution, referring to the amount of time replaced in the traditional workplace; and the diversity of employment relationships between employer and employee, ranging from contract work to traditional full-time employment

‣A frequently repeated motto is that "work is something you do, not something you travel to." Variations of this include: "Work is something we DO, not a place that we GO" and "Work is what we do, not where we are.

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.

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.

8.3 The Digital Divide:

Q. What is being done to reduce the negative influences of the Digital divide? W/13, S/14 W/14 CSE W/13 S/ 14 IT W/14 S/15 IT

The term *Digital divide* describes a gap between those who have ready access to information and communication technology and the skills to make use of those technology and those who do not have the access or skills to use those same technologies within a geographic area, society or community. It is an economic and social inequality between groups of persons.

Conceptualization of the digital divide has been described as follows:

- Subjects who have connectivity, or who connects: individuals, organizations, enterprises, schools, hospitals, countries, etc.
- Characteristics of connectivity, or which attributes: demographic and socio-economic variables, such as income, education, age, geographic location, etc.
- Means of connectivity, or connectivity to what: fixed or mobile, Internet or telephony, digital TV, etc.
- Intensity of connectivity, or how sophisticated the usage: mere access, retrieval, interactivity, innovative contributions.

- Purpose of connectivity, or why individuals and their cohorts are (not) connecting: reasons individuals are and are not online and uses of the Internet and information and communications technologies ("ICTs").
- Dynamics or evolution, whether the gap of concern will increase or decrease in the future, when the gap of concern would be maximized

When people talk about standard of living, they are often referring to a level of material comfort measured by the goods, services, and luxuries available to a person, group, or nation—factors beyond the GDP-based measurement of standard of living. Some of these indicators are:

• Average number of calories consumed per person per day

• Availability of clean drinking water

• Average life expectancy

• Literacy rate

• Availability of basic freedoms

• Number of people per doctor

• Infant mortality rate

• Crime rate

• Rate of home ownership

• Availability of educational opportunities

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 shows up clearly when one examines the rates of PC ownership and Internet use in various countries around the world

8. 4 THE IMPACT OF IT ON HEALTH CARE COSTS:

Q. How the use of electronic health records can improve patient health care and reduce costs? Explain with example W/13 W/14 CT

‣The rapidly rising cost of health care is one of the major challenges of the 21st century.

‣The United States spent an estimated $2.4 trillion on health care in 2008 versus $1.7 trillion in 2003.

‣The share of gross domestic product spent on national health care has grown from 7.2 percent in 1970 to an estimated 16.6 percent in 2008.

‣Current estimates are that national healthcare spending will more than double to over $4 trillion per year by 2016, with one out of every five dollars spent in the United States going toward health care.

‣The development and use of new medical technology, such as new diagnostic procedures and treatments 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.

‣ In addition, even if new procedures and treatments cost less (for example, magnetic resonance imaging), they may stimulate much higher rates of use because they are more effective or cause less discomfort to patients.

‣Patients sometimes overuse medical resources that appear to be free or almost free thanks to the share of medical bills that is paid by third parties, such as insurance companies and government programs.

‣ A patient who doesn’t have to pay for a medical test or procedure is probably less likely to consider its cost-to-benefit ratio.

‣Attempts by insurance companies to rein in those costs have led to a blizzard of paperwork but have proven ineffective.

‣really gain control over soaring healthcare costs, patient awareness must be raised and technology costs must be managed more carefully. In the meantime, however, the improved use of IT in the healthcare industry can lead to significant cost reductions in a number of ways.

8.5 Electronic Health Records:

Q. . Explain in Details electronic health record with example. W/14 , S/14 CSE W/14 IT

‣Although the healthcare industry depends on highly sophisticated technology for diagnostics and treatment, it has been slow to implement IT solutions to improve productivity and efficiency.

‣The healthcare industry invests about $3,000 in IT for each worker, compared with about $7,000 per worker in private industry generally and nearly $15,000 per worker in the banking industry.

‣One tremendous opportunity for improving health care through the use of IT is in the process of capturing and recording patient data.

‣Before seeing a physician, many patients are given a clipboard and pen with a standard form to complete. Some people must wonder: “This is the same form I filled out last time; what did they do with the data from my last visit?”

‣It is nearly impossible to pull together the paper trail created by a patient’s interactions with various healthcare entities to create a clear, meaningful, consolidated view of that person’s health history.

‣This lack of patient data transparency can result in diagnostic and medication errors as well as the ordering of duplicate tests, which dramatically increase healthcare costs. It can even compromise patient safety.

‣For example, physicians in the emergency room must often treat a patient who is unconscious and incapable of providing essential medical information, such as the name of his or her primary care physician, information about recent illnesses or surgeries, medications taken, allergies, and other useful data.

‣Without such data, the ER physician is essentially taking a gamble in treating the patient. If the United States had a comprehensive healthcare information network, such medical data could be readily available for all patients at any medical facility.

‣A 1999 report by the Institute of Medicine (IOM) found that as many as 98,000 Americans die annually due to preventable medical errors. In addition, a 2006 IOM report concluded that more than 1.5 million preventable medication errors per year cost the United States about $3.5 billion annually.

‣A 2009 Consumers Union report claims that we have made no real progress toward reducing the number of deaths. However, as far back as 2004, healthcare experts agreed that“going digital”could eliminate many of these needless deaths.

‣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 A study based on data collected in 2008 revealed that of the 3,000 U.S. hospitals surveyed, less than 2 percent use comprehensive EHRs and only about 8 percent use basic EHRs.

‣Effective use of EHR systems has been shown to improve patient care and reduce costs.

‣In a Commonwealth Fund study of 41 Texas hospitals that treat a diverse group of patients suffering from a variety of medical conditions, researchers found that a 10 percent increase in the use of electronic notes and medical records was associated with a 15 percent reduction in the likelihood of patient death.

‣When physicians electronically entered patient care instructions; there was a 55 percent reduction in the likelihood of death related to some procedures.

8. 6 Use of Mobile and Wireless Technology in the Healthcare Industry:

Q. How can make use of mobile and how are they employed in the IT industry? W/14 CSE S/14 IT W/14 IT S/15 CT

Although slow to invest in IT, the healthcare industry was actually a leader in adopting mobile and wireless technology, perhaps because of the frequent urgency of communications with doctors and nurses who are almost always on the move. For example, doctors were among the first large groups to start using PDAs on the job. Other 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

8.7 Telemedicine:

Q. Define Telemedicine illustrate store and forward telemedicine and live telemedicine. W/13 IT W/14 IT S/15 CT

‣Telemedicine employs modern telecommunications and information technologies to provide medical care to people who live far away from healthcare providers.

‣ This technology reduces the need for patients to travel for treatment and allows healthcare professionals to serve more patients in a broader geographic area.

‣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.

‣This type of monitoring does not require the presence of the patient and care provider at the same time, and having access to such information can enable healthcare professionals to recognize problems and intervene before high-risk situations become life threatening.

‣ for example, patients who have chronic diseases often don't recognize early warning signs that indicate an impending health crisis. A sudden weight gain by a patient who has suffered

congestive heart failure could indicate retention of fluids, which could lead to a traumatic trip to the emergency room or even loss of life.

‣A physician who uses telemedicine to keep tabs on such patients could make a vital difference. Live telemedicine are quires the presence of patients and healthcare providers at the same time and often involves a video conference link between the two sites.

‣The University of Rochester's Golisano Children's Hospital in New York uses the Health-e-Access telemedicine program to screen children in inner-city schools for asthma.

‣The use of telemedicine does raise some new issues. Must the physicians providing advice to patients at a remote location be licensed to perform medicine at that location— perhaps a different state or country? Must a healthcare system be required to possess a license from a state in which it has a"virtual"facility, such as a video conferencing room? Will the various states require some form of assurance that minimum technological standards .

University Ques:

Q. Comment On Ethical issue in " Because some entitles can afford to make significant investment in IT while others cannot and thus are blocked in their efforts to raise productivity. W/13 CSE

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.

▪For example, productivity in a factory might be measured by the number of labor hours it takes to produce one item, while productivity in a service sector company might be measured by the annual revenue an employee generates divided by the employee's annual salary.

▪ Most countries have continually been able to produce more goods and services over time—not through a proportional increase in input but by making production more efficient.

▪These gains in productivity have led to increases in the GDP-based standard of living because the average hour of labor produced more goods and services.

▪ The Bureau of Labor Statistics tracks U.S. productivity on a quarterly basis. In the United States, labor productivity growth has averaged about 2 percent per year for the past century, meaning that living standards have doubled about every 36 years.

▪ Innovation is a key factor in productivity improvement, and IT has played an important role in enabling innovation.

▪Progressive management teams use IT, as well as other new technology and capital investment, to implement innovations in products, processes, and services.

▪In the early days of IT in the 1960s, productivity improvements were easy to measure. For example, midsized companies often had a dozen or more accountants focused solely on payroll-related accounting.

▪When businesses learned to apply automated payroll systems, fewer accounting employees were needed. The productivity gains from such IT investments were obvious.

▪Today, organizations are trying to further improve IT systems and business processes that have already gone through several rounds of improvement.

▪Organizations are also adding new IT capabilities to help workers who already have an assortment of personal productivity applications on their desktop computers, laptops, and personal digital assistants (PDAs).

▪Instead of eliminating workers, companies are saving workers small amounts of time each day. Whether these saved minutes actually result in improved worker productivity is a matter for debate.

▪ Many analysts argue that workers merely use the extra time to do some small task they didn't have time to do before, such as respond to e-mail they would have ignored.

▪These minor gains make it harder to quantify the benefits of today's IT investments on worker productivity.

Q. Explain medical information on website for laypeople. W/14 IT

▪Medical Information Websites provides many informations concerning different medical topics to learn more about healthcare services and new developments in medicines.
▪ **Laypeople** can't become as informed as trained medical practitioner, but the presence of many Medical Information is already available by the use of the web.
▪*A web presence provides details on patient care, disease information, new development in medicines, preventions for common ailments, proper treatment and other information regarding to some certain diseases.*

▪*Medical Information website* also include informations not only for patients but also for all visitors such as office hours, interactive maps with directions to the facilities and hospitals, patient acceptance policies, appointment and billing contacts, they also provide information related, of course, to health such as family and group practices, plastic and cosmetic surgery, optical surgery, physical therapy, informations related to dentistry, pharmacies, medical labs and even ambulatory services.

▪Web Solution is linked to other medical organizations on the internet and more than **20%** of all internet traffic is health-related in content based on the computer industry.

▪ Many Websites links to other websites provide the ideal starting point for patients to obtain the medical information they are looking for.

▪ And they keep on helping and encouraging many people, especially patients to go online to compare the quality, safety and cost information on hospitals nationwide and to know the average prices of drugs and treatment options available nationwide.

▪*And these many health information websites should be responsible for capturing and updating data as needed to provide accurate and current medical information.*

Q Short note on 1) E-RATE PROG 2) ONE LAPTOP PER CHILD (OLPC) 3) CLASS-MATE 4) E-LAPTOP

E-Rate

▪**E-Rate** is the commonly used name for the Schools and Libraries Program of the Universal Service Fund, which is administered by the Universal Service Administrative Company (USAC) under the direction of the Federal Communications Commission (FCC).

▪The program provides discounts to assist schools and libraries in the United States to obtain affordable telecommunications and Internet access.

▪It is one of four support programs funded through a Universal Service fee charged to companies that provide interstate and/or international telecommunications services.

Function

▪The Schools and Libraries Program supports connectivity - the conduit or pipeline for communications using telecommunications services and/or the Internet.

▪Funding is requested under four categories of service: telecommunications services, Internet access, internal connections, and basic maintenance of internal connections.

▪Discounts for support depend on the level of poverty and the urban/rural status of the population served and range from 20% to 90% of the costs of eligible services. Eligible schools, school districts and libraries may apply individually or as part of a consortium.

▪Applicants must provide additional resources including end-user equipment (e.g., computers, telephones, etc.), software, professional development, and the other elements that are necessary to utilize the connectivity funded by the Schools and Libraries Program.

One Laptop per Child

One Laptop per Child (OLPC) was setup to oversee the creation of affordable educational devices for use in the developing world.

Its primary goal is the production and distribution of the OLPC XO, a low-cost and low-power laptop computer. The project was originally funded by member organizations such as AMD, Chi Mei, eBay, Google, Marvell Technology Group, News Corporation, Nortel, Red Hat, and Quanta.

The OLPC project has received criticism both specific to its mission, and criticism that is typical of many such systems, such as support, ease-of-use, security, content-filtering and privacy issues. Officials in some countries have criticized the project for its appropriateness in terms of price, cultural emphasis and priority as compared to other basic needs of people in third-world settings.

CLASS-MATE+:

1) In 2006 Intel introduced a low cost laptop called class mate pc. The first generation of this notebook computer cost under $400 and was designed for use in kindergarten through high school classroom in developing countries.

2)Intel does not manufacture the computers but provides free blueprints to manufacturers and independent dealers.

3) The computer began shipping in early 2007 to 25 countries, including Brazil, chile, Nigeria, China India . Since then Intel and Lenovo have patterned to introduce the classmate + laptop targeted for sale bulk quantities.

Eee Laptop:

1)Asustek computer, Inc is a Taiwanese multinational manufacturer of computer and computer components. Its Eee Pad Transformer computer is a tablet computer that can convert into a laptop with the addition of an optional keyboard.

2) The device is priced at $399 or about $100 less than the apple i-pad t5ablet computer. At This price , the computer is a competitor to the OLPC AND Intel classmate + for widespread deployment in developing countries.

9 SOCIAL NETWORKING

9. WHAT IS A SOCIAL NETWORKING WEB SITE?

Q. How Social networking website, how do people use them and what are some of their practical business use? W/13, S/14 , S/15 CSE

‣A social networking Web site is a site whose purpose is to create an online community of Internet users that enables members to break down barriers created by time, distance, and cultural differences.

‣Social networking Web sites allow people to interact with others online by sharing opinions, insights, information, interests, and experiences.

‣Members of an online social network may use the site to interact with friends, family members, and colleagues—people they already know—but they may also wish to develop new personal and professional relationships.

‣With over 1.6 billion Internet users, there is an endless range of interests represented online, and a correspondingly wide range of social networking Web sites catering to those interests.

‣In the United States, total minutes per month spent on social networking Web sites increased 83 percent from April 2008 to April 2009.

‣ Total minutes on Face book grew from 1.7 billion in April 2008 to 13.9 billion in April 2009, making Face book the number one social networking Web site when ranked by total minutes per month.

‣There are thousands of social networking Web sites worldwide

Social networking Web site	Description	Number of unique visitors in January 2009
Facebook.com	Largest social networking Web site based on the number of unique visitors per month; used by members to keep up with friends, upload photos, share links and videos, and learn more about the people they meet	69 million
MySpace.com	General social networking Web site used by teenagers and adults worldwide; designed to allow members to communicate with friends via personal profiles, blogs, and groups, as well as post photos, music, and videos to their personal pages	59 million
Classmates.com	Networking site designed to help members find and keep in touch with people they knew in grade school, high school, college, and the military	17 million
Reunion.com	Site that helps members find and keep in touch with old friends, relatives, and loved ones	14 million
LinkedIn.com	Business-oriented Web site used for professional networking; users create a network made up of people they know and trust in business	11 million
imeem.com	Music sharing site that enables members to watch video clips, stream music, view photos, post to blogs and forums, join groups, and browse profiles	9 million

9.1 BUSINESS APPLICATIONS OF ONLINE SOCIAL NETWORKING:

While social networking Web sites are primarily used for non business purposes, a number of forward-thinking organizations are employing this technology to advertise, assess job candidates, and sell products.

9.1.1 Social Network Advertising:

‣**Social network advertising**, also **social media targeting** is a group of terms that are used to describe forms of online advertising that focus on social networking services.

‣One of the major benefits of this type of advertising is that advertisers can take advantage of the users' demographic information and target their ads appropriately.

‣Social media targeting combines current targeting options (like geo targeting, behavioral targeting, socio-psychographic targeting, etc.), to make detailed target group identification possible.

‣With social media targeting, advertisements are distributed to users based on information gathered from target group profiles.

‣Social network advertising is not necessarily the same as social media advertising.

‣Social media targeting is a method of optimizing social media advertising by using profile data to deliver advertisements directly to individual users. Social media targeting refers to the process of matching social network users to target groups that have been specified by the advertiser.

9.1.2 Application

‣People who use social networks store various information about them including, but not limited to, their age, gender, interests and location.

‣This stored information allows advertisers to create specific target groups and individualize their advertisements.

‣The advantage for advertisers is that their ads can reach people who are interested in the product or service.

‣ The advantage for users is that they can see ads that appeal to them. Face book, for example, the hugely popular social network, has developed a targeting technology which allows advertisements to reach a specific audience.

‣This is why Face book users see advertisements on their profile page that are tailored to their gender, music taste, or location.

9.1.3 Types of Advertising

‣Popular social media sites, Face book, Twitter, and YouTube, offer different ways to advertise brands. Face book gives advertisers options such as promoted posts, sponsored stories, page post ads, Face book object (like) ads, and external website (standard) ads.

‣ To advertise on Twitter there are promoter tweets, trends, and promoted accounts that show up on users newsfeeds. For advertising on YouTube there are branded channels, promoted videos, an in video advertising.

9.1.4 Advantages

- Advertisers can reach users who are interested in their products
- Allows for detailed analysis and reporting (including Business Intelligence)
- The information gathered is real, not from statistical projections

- Does not access IP-Addresses of the users

9.1.5 There are several social network advertising strategies, and organizations may employ one or more of the following:

Q. Discuss several social network advertising strategies. W/13 , S/14 CT S/14 CSE

9.1.5.1 Direct Advertising

Direct advertising involves placing banner ads on a social networking Web site. An ad can either be displayed to each visitor to the Web site or, by using the information in user profiles, be directed toward those members who would likely find the product most appealing. Thus, an ad for a new magazine on mountain biking could be directed to individuals on a social networking Web site who are male, who are 18 to 35 years old, and who express an interest in mountain biking. Others on the social networking Web site would not see it

9.1.5.2 Advertising Using an Individual's Network of Friends

Companies can use social networking Web sites to advertise to an individual's network of contacts. When you sign on to your favorite social networking Web site, you might see a message saying,"Jared [your friend] just went to see Transformers II—awesome, he says!"

This can be an extremely believable message, as people frequently make decisions to do something or purchase something based on input from their close group of friends. This might be a spontaneous message sent by Jared, or Jared might be getting paid by an online promotion firm to send messages about certain products. There are certainly ethical issues with this approach, as some people consider this to be exploiting an individual's personal relationships for the financial benefit of a company.

9.1.5.3Indirect Advertising Through Groups

Innovative companies are also making use of a new marketing technique by creating a group on a social networking Web site that interested users can join by becoming"fans."These groups can quickly grow in terms of numbers of fans to become a very effective marketing tool for a company looking to market contests, promote new products, or simply increase brand awareness.

9.1.5.4 Company-Owned Social Networking Web Site

A variation on the above approach is for a company to form its own social networking Web site. Dell created its own social networking Web site, Idea Storm, as a means for its millions of customers in more than 100 countries to talk about what new products, services, or improvements they would like to see Dell develop. Since its launch in February 2007, the Dell community has suggested 11,996 ideas and posted 84,851 comments; Dell has implemented 350 customer-submitted ideas.

9.1.5.5 Viral Marketing

‣Viral marketing encourages individuals to pass along a marketing message to others, thus creating the potential for exponential growth in the message's exposure and influence as one person tells two people, each of those two people tell two or three more people, and so on.

‣The goal of a viral marketing campaign is to create a buzz about a product or idea that spreads wide and fast. A successful viral marketing campaign requires little effort on the part of the advertiser; however, the success of such campaigns can be very difficult to predict.

‣Hotmail created what is recognized by many as the most successful viral marketing campaign ever when it first launched its service in 1996. Every e-mail sent by a Hotmail user contained a short message at the end of the e-mail that promoted Hotmail's free e-mail service. As a result, almost 12 million new users signed up for Hotmail over a period of 18 months.

9.1.5.6 Social Shopping Web Sites

‣A social shopping Web site brings shoppers and sellers together in a social networking environment in which members can share information and make recommendations while shopping online.

‣Thus, these sites combine two highly popular online activities—shopping and social networking. Social shopping Web site members can typically build their own pages to collect information and photos about items in which they are interested.

‣On many social shopping Web sites, users can offer opinions on other members' purchases or potential purchases.

‣The social shopping Web site Stuff pit has implemented a reward system for members, in which they are paid a commission each time another shopper acts on their recommendation to purchase a specific item

Sample of social shopping Web sites

Social shopping site	Brief description
Buzzillions	Product review Web site that collects thousands of product reviews from the Web sites of various retailers
Crowdstorm	Shopping resource that aggregates product information from various online buyers guides, reviews, and blog postings
Kaboodle	Site where members can discover and recommend new products; get discounts; and locate bargains
OSOYOU	UK-based social shopping site for women with an interest in fashion and beauty products
ZEBO	Site that allows members to create a personal profile about what they own, want, and love to shop for; members can check out one another's profiles, provide shopping tips, and chat online to ask questions and get advice

‣Social shopping Web sites generate revenue through retailer advertising. Some also earn money by sharing with retailers data about their members' likes and dislikes.

‣Social shopping Web sites can be a great way for small businesses to boost their sales. Amenity Home—a tiny start-up with just three products, four employees, and no advertising budget—became a retailer on ThisNext.com, a social shopping Web site whose goal is to link shoppers with hard-to-find products.

‣Shoppers at ThisNext.com found the Amenity Home products, copied photos of the products to their own blog pages, and brought the tiny firm some much-needed

recognition—Amenity Home products started getting more and more hits on ThisNext.com.

‣Retailers can purchase member data and comments from some social shopping Web sites to find out what consumers like and don't like, and what they are looking for in items sold by the retailer. This can help the retailer design product improvements and come up with ideas for new product lines

9.2 SOCIAL NETWORKING ETHICAL ISSUES:

When you have a community of tens of millions of users, not everyone is going to be a good "neighbor"and abide by the rules of the community. Many will stretch or exceed the bounds of generally accepted behavior. Some of the common ethical issues that arise for members of social networking Web sites are **cyberbullying**, **cyberstalking,** encounters with sexual predators, and the uploading of inappropriate material

9.2.1 Cyber bullying

Q. Short note on Cyber-bullying W/13, S/15 CSE

Cyber bullying is the harassment, torment, humiliation, or threatening of one minor by another minor or group of minors via the Internet or cell phone. According to a recent survey of over 800 students ages 13–17, about 43 percent had experienced cyber bullying in the past year. Cyber bullying is more common among females and among 15- and 16-year-olds.

Cyber bullying is the use of social networks to repeatedly harm or harass other people in a deliberate manner. According to U.S. Legal Definitions, "cyber-bullying could be limited to posting rumors or gossips about a person in the internet bringing about hatred in other's minds; or it may go to the extent of personally identifying victims and publishing materials severely insult and embarrassing them.

Legal definition

Cyber bullying is defined in legal glossaries as

- actions that use information and communication technologies to support deliberate, repeated, and hostile behavior by an individual or group, that is intended to harm another or others.
- use of communication technologies for the intention of harming another person
- use of internet service and mobile technologies such as web pages and discussion groups as well as instant messaging or SMS text messaging with the intention of harming another person.

Examples of what constitutes cyber bullying include communications that seek to intimidate, control, manipulate, put down, falsely, or humiliate the recipient. The actions are deliberate, repeated, and hostile behavior intended to harm another. Cyber bullying has been defined by The National Crime Prevention Council: "When the Internet, cell phones or other devices are used to send or post text or images intended to hurt or embarrass another person." A cyber bully may be a person whom the target knows or an online stranger. A cyber bully may be anonymous and may solicit involvement of other people online who do not even know the target. This is known as a "digital pile-on." Cyber bullying has been defined as "when the Internet, cell phones or other devices are used to send or post text or images intended to hurt or embarrass another person".

There are numerous forms of cyber bullying, such as the following:

• Sending mean-spirited or threatening messages to the victim

• Sending thousands of text messages to the victim's cell phone and running up a huge cell phone bill

• Impersonating the victim and sending inappropriate messages to others

• Stealing the victim's password and modifying his or her profile to include racist, homophobic, sexual, or other inappropriate data that offends others or attracts the attention of undesirable people

• Posting mean, personal, or false information about the victim in the cyberbully's blog

• Creating a Web site whose purpose is to humiliate or threaten the victim

• Taking inappropriate photos of the victim and either posting them online or sending them to others via cell phone

• Setting up an Internet poll to elicit responses to embarrassing questions, such as"Who's the biggest geek in Miss Adams's homeroom?"and"Who is the biggest loser in the senior class?"

• Sending inappropriate messages while playing interactive games that enable participants to communicate with one another.

9.3 Cyber stalking:

Q. What will you do if you become a victim of cyber stalking? w/13 W/14 CT W/13, S/15 CSE

‣**Cyber stalking** is the use of the Internet or other electronic means to stalk or harass an individual, a group, or an organization.

‣It may include false accusations, defamation, slander and libel. It may also include monitoring, identity theft, threats, vandalism, solicitation for sex, or gathering information that may be used to threaten or harass.

‣Cyber stalking is often accompanied by real time or offline stalking. Both are criminal offenses. Both are motivated by a desire to control, intimidate or influence a victim.

‣ A stalker may be an online stranger or a person whom the target knows. He may be anonymous and solicit involvement of other people online who do not even know the target.

‣Cyberstalking is a criminal offense under various state anti-stalking, slander and harassment laws. A conviction can result in a restraining order, probation, or criminal penalties against the assailant, including jail.

9.3.1 A number of key factors have been identified in cyber stalking:

- **False accusations**. Many cyber stalkers try to damage the reputation of their victim and turn other people against them. They post false information about them on websites. They may set up their own websites, blogs or user pages for this purpose. They post allegations about the victim to newsgroups, chat rooms, or other sites that allow public contributions such as Wikipedia or Amazon.com.
- **Attempts to gather information about the victim**. Cyber stalkers may approach their victim's friends, family and work colleagues to obtain personal information. They may advertise for information on the Internet, or hire a private detective.
- **Monitoring their target's online activities** and attempting to trace their IP address in an effort to gather more information about their victims.
- **Encouraging others to harass the victim**. Many cyber stalkers try to involve third parties in the harassment. They may claim the victim has harmed the stalker or his/her family in some way, or may post the victim's name and telephone number in order to encourage others to join the pursuit.
- **False victimization**. The cyber stalker will claim that the victim is harassing him/her.
- **Attacks on data and equipment**. They may try to damage the victim's computer by sending viruses.
- **Ordering goods and services**. They order items or subscribe to magazines in the victim's name. These often involve subscriptions to pornography or ordering sex toys then having them delivered to the victim's workplace.
- **Arranging to meet**. Young people face a particularly high risk of having cyber stalkers try to set up meetings between them.[14]

9.4 Cyber bullying vs. cyber stalking

‣The practice of cyber bullying is not limited to children and, while the behavior is identified by the same definition when practiced by adults, the distinction in age groups sometimes refers to the abuse as cyber stalking or cyber harassment.

‣ when perpetrated by adults toward adults. Common tactics used by cyber stalkers are performed in public forums, social media or online information sites and are intended to threaten a victim's earnings, employment, reputation, or safety.

‣Behaviors may include encouraging others to harass the victim and trying to affect a victim's online participation.

‣Many cyber stalkers try to damage the reputation of their victim and turn other people against them.

‣Cyber stalking may include false accusations, monitoring, making threats, identity theft, damage to data or equipment, the solicitation of minors for sex, or gathering information in order to harass.

‣A repeated pattern of such actions and harassment against a target by an adult constitutes cyber stalking.

‣Cyber stalking often features linked patterns of online and offline behavior.

‣There are consequences of law in offline stalking and online stalking, and cyber stalkers can be put in jail. Cyber stalking is a form of cyber bullying

9.5 Uploading of Inappropriate Material:

Q. How social networking websites manage the uploading of inappropriate material? S/14 CT W/13 CSE S/15 CT S/15 CSE

‣Most social networking Web sites have policies against uploading videos depicting violence or obscenity.

‣Facebook, MySpace, and most other social networking Web sites have terms of use agreements, a privacy policy, or a content code of conduct that summarizes key legal aspects regarding use of the Web site.

‣Typically, the terms state that the Web site has the right to delete material and terminate user accounts that violate the site's policies.

‣The policies set specific limits on content that is sexually explicit, defamatory, hateful, or violent, or that promotes illegal activity.

‣Policies do not stop all members of the community from attempting to post inappropriate material, and most Web sites do not have sufficient resources to review all material submitted for posting.

‣ For example, about 10 hours of media is being uploaded to YouTube every minute. Quite often, it is only after other members of a social networking Web site complain about objectionable material that such material is taken down.

‣This can be days or even weeks. Ideally, reviewers would also look at the text content submitted to a networking site—not just photos and videos.

‣ A posting to a teenage-oriented Web site may advocate underage drinking, sex, and drug use without the use of photos or videos.

‣Individuals who appear in photos or videos doing inappropriate things may find themselves in trouble with authorities if those photos and videos end up on the Internet.

‣ In April 2008, six teenagers recorded their beating of 16-year-old Victoria Lindsay and planned to post the video on MySpace and YouTube.

‣ The beating was severe enough that Victoria suffered temporary damage to her sight and hearing. According to YouTube, the video was never uploaded, and a YouTube spokesperson stated that "if a video shows someone getting hurt, attacked, or humiliated, it will be removed."

‣A MySpace employee confirmed that the video was never uploaded to that site. MySpace has a dedicated content review team that views every video before it is posted to ensure that the poster is not violating the MySpace terms of use.

9.6 ONLINE VIRTUAL WORLDS

‣An online virtual world is a computer-simulated world in which a visitor can move in three-dimensional space, communicate and interact with other visitors, and manipulate elements of the simulated world.

‣Virtual worlds are usually thought of as alternative worlds where visitors go to entertain themselves and interact with others. A visitor to a virtual world represents him- or herself through anavatar.

‣a character usually in the form of a human but sometimes in some other form.

‣Avatars can typically communicate with each other via text chat or via voice using Voice over IP Avatars in many virtual worlds can shop, hold jobs, run for political office, develop relationships with other avatars, take a test drive in a virtual world car, and even engage in criminal activities.

‣ Avatars may promote events and hold them in the virtual world (e.g., garage sales or concerts). Avatars can even start up new businesses and create or purchase new entities, such as houses, furnishings for their houses, clothing, jewelry, and other products

‣Avatars use the virtual world's currency to purchase goods and services in the virtual world. The ownership of such items is recognized by other avatars in the virtual world—for example,this is John's house; others may not occupy it without his permission.

‣Avatars can earn virtual world money by performing tasks in the virtual world, or their owners can purchase virtual world money for them using real world cash.

‣ In some virtual worlds, avatars can convert their virtual world money back into real dollars at whatever the going exchange rate is by using their credit card at online currency exchanges.

‣Virtual world items may also be sold to other virtual world players for real world money. A virtual world may also support e-commerce and allow users to sell their own real products (e.g., autos and time-share vacations) within the real world.

‣Most virtual worlds have rules against offensive behavior in public, such as using racial slurs or performing overtly sexual actions.

‣However, consenting adults can travel to private areas and engage in all sorts of socially unacceptable behavior.

9.7 Rejecting a job allocation based on the content of the individual social N/W profile

Q. Briefly discuss the legality of an employer rejecting a job allocation based on the content of the individual social N/W profile W/14, S/15 CT

▪Employers can and do look at the social networking profiles of job candidates when making hiring decisions .

▪According to a recent survey by CareerBuilder.com, 22 percent of hiring managers use social networking Web sites as a source of information about candidates, and an additional 9 percent are planning to do so. Of those managers who use social networking Web sites to screen candidates, 34 percent have found information that made them drop a candidate from consideration.

▪Companies may reject candidates who post information about their drinking or drug use habits or those who post provocative or inappropriate photos.

▪Candidates are also sometimes rejected due to postings containing discriminatory remarks relating to race, gender, and religion or because of postings that reveal confidential information from previous employers.

▪Employers can legally reject a job applicant based on the contents of the individual's social networking profile as long as the company is not violating federal or state discrimination laws.

▪For example, an employer cannot legally screen applicants based on race or ethnicity. Or suppose that by checking a social networking Web site, a hiring manager finds out that a job candidate is pregnant and makes a decision not to hire that person based on that information.

▪Refusing to hire on the basis of pregnancy is prohibited by the Pregnancy Discrimination Act, which amended Title VII of the Civil Rights Act of 1964.

▪ The employer would be at risk of a job employment discrimination lawsuit.

▪Members of social networking Web sites frequently provide sex, age, marital status, sexual orientation, religion, and political affiliation data in their profile.

▪Users who upload personal photos may reveal a disability or their race or ethnicity; therefore, without even thinking about it, an individual may have revealed data about personal characteristics that are protected by civil rights legislation.

▪ Some human resource executives feel that they can use social networking Web sites to"learn a little about the candidate's cultural fit and professionalism."

▪Another survey done by CollegeGrad.com revealed that 47 percent of college graduates who use social networking Web sites change the contents of their pages as a result of their job search.

▪Many jobseekers delete their Facebook or MySpace account altogether because they know employers check such sites.

▪More graduates are beginning to realize that pictures and words posted online, once intended for friends only, are reaching a much larger audience and could have an impact on their job search.

Chapter 10

ETHICS OF IT ORGANIZATIONS

10. KEY ETHICAL ISSUES FOR ORGANIZATIONS:

‣The use of nontraditional workers, including temporary workers, contractors, consulting firms, H-1B visa workers, and outsourced offshore workers, gives an organization more flexibility in meeting its staffing needs, often at a lower cost.

‣The use of nontraditional workers also raises ethical issues for organizations. When should such nontraditional workers be employed, and how does such employment affect an organization's ability to grow and develop its own employees? How does the use of such resources impact the wages of the organization's employees?

• 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. It is an important ethical issue for individuals and organizations. How does one safely and effectively report misconduct, and how should managers handle a whistle-blowing incident?

• 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. What has been done so far, and what still needs to be done.

10.1 CONTINGENT WORKERS:

Q. Advantage & Disadvantage of Contingent workers S/14 CT W/13 IT S/15 CT
Q. Discuss consideration involved in deciding whether or not to hire contingent worker. W/14 CT
Q. What are contingent workers and how are they employed in the IT industry? W/13 S/14 W/14 CSE W/13 , S/14, W/14 IT

‣Companies use contingent workers for job situations in which an individual does not have an explicit contract for long-term employment.

‣Contingent workers include independent contractors and temporary workers.

‣Companies use contingent workers when they have an increased need for personnel.

‣ Temporary staffing firms recruit, train and test job seekers in large range of job skills. ▪Temporary work appeal to most people who want and/ or need the flexibility in their work schedule.

‣This also gives them more job experience; this means employees may have more skills.

‣Employers sometimes transfers all or part of its workforce to another firm. The leasing firm handles all human resources related activities and costs.

‣Business also obtain employees from consulting firm.

There are advantages to using contingent employees

- Firm does not have to provide benefits
- Can easily adjust the number of workers
- Can easily release workers.
- Contingent workers may already be specialist

Disadvantages for using Contingent workers

- Contingent workers may not feel strong connection to the company.
- Skills employees gain from projects is lost to the company when the leave.

10.2 H-1B Workers

Q. Describe the process of H-1B application W/13 & S/14 CT S/14 IT
Q. What key ethical issue is associated with the use of contingent workers, including H-1b visa holders and offshore outsourcing companies? W/13 S/14, W/14 CSE W/14 IT
Q. Define H-1B visa. Enlist various steps in H-1 B application process w/13 IT S/15 CSE

- H-1B is a temporary work visa granted by the USCIS.
- These people work specialty jobs that require at least a four year bachelor's degree (in the USA, 3 years elsewhere) in a specific field. An H1B worker is allowed to work for 6 years then they must leave the U.S.
- For one year before they can be allowed to petition for another visa. H1B workers make up only 0.1% of the U.S. almost 40% of them are employed in the IT industry.

Application process

The process of getting a H-1B visa has three stages:

- The employer files with the United States Department of Labor a Labor Condition Application (LCA) for the employee, making relevant attestations, including attestations about wages (showing that the wage is at least equal to the prevailing wage and wages paid to others in the company in similar positions) and working conditions.
- With an approved LCA, the employer files a Form I-129 (Petition for a Nonimmigrant Worker) requesting H-1B classification for the worker. This must be accompanied by necessary supporting documents and fees.
- Once the Form I-129 is approved, the worker may begin working with the H-1B classification on or after the indicated start date of the job, if already physically present in the United States in valid status at the time.
- If the employee is outside the United States, he/she may use the approved Form I-129 and supporting documents to apply for the H-1B visa. With a H-1B visa, the worker may present himself or herself at a United States port of entry seeking admission to the United States, and get an Form I-94 to enter the United States.
- Employees who started a job on H-1B status without a H-1B visa because they were already in the United States still need to get a H-1B visa if they ever leave and wish to reenter the United States while on H-1B status.

10.3 OUTSOURCING:

Q. What is outsourcing? Discuss advantage and disadvantage of offshore outsourcing **W/14 CSE S/14 IT**

•Outsourcing is a long-term business arrangement in which a company contracts for services with an outside organization that has expertise in providing a certain function.

•The outside organization may perform the following services operating data center, support for telecommunications network, or staffing a help-desk.

•The reason for outsourcing is to lower costs and strategic flexibility. Offshore outsourcing is the outsourcing of jobs to organization who employees live in a foreign country.

10.3.1 Reasons for outsourcing

•Companies primarily outsource to reduce certain costs — such as peripheral or "non-core" business expenses, high taxes, high energy costs, excessive government regulation/mandates, production and/or labor costs.

•The incentive to outsource may be greater for U.S. companies due to unusually high corporate taxes and mandated benefits, like social security, Medicare, and safety protection (OSHA regulations) At the same time, it appears U.S. companies do not outsource to reduce executive or managerial costs.

• For instance, executive pay in the United States in 2007 was more than 400 times more than average workers—a gap 20 times bigger than it was in 1965.[19] In 2011, twenty-six of the largest US corporations paid more to CEO's than they paid in federal taxes.[20] Such statistics imply that the reason companies outsource is not to avoid costs in general but to avoid specific types of costs

10.4 Offshore outsourcing

‣**Offshore outsourcing** is the practice of hiring an external organization to perform some business functions ("Outsourcing") in a country other than the one where the products or services are actually developed or manufactured ("Offshore").

‣It can be contrasted with offshoring, in which a company moves itself entirely to another country, or where functions are performed in a foreign country by a foreign subsidiary.

‣Opponents point out that the practice of sending work overseas by countries with higher wages reduces their own domestic employment and domestic investment.

‣ Many customer service jobs as well as jobs in the information technology sectors (data processing, computer programming, and technical support) in countries such as the United States and the United Kingdom - have been or are potentially affected.

10.4.1 Types

There are four basic types of offshore outsourcing:

- ITO — Information Technology Outsourcing
- BPO — Business Process Outsourcing
- Software R&D — offshore software development
- KPO - Knowledge Process Outsourcing

10.4.2 Criteria

The general criteria for a job to be offshore-able are:

- There is a significant wage difference between the original and offshore countries;
- The job can be telework;
- The work has a high information content;
- The work can be transmitted over the Internet;
- The work is easy to set up;

- The work is repeatable.

The driving factor behind the development of offshore outsourcing has been the need to cut costs while the enabling factor has been the global electronic internet network that allows digital data to be accessed and delivered instantly, from and to almost anywhere in the world.

10.4.3 Pros and Cons of Offshore Outsourcing

From factories moving operations overseas to technical support phone banks in India, outsourcing is a part of everyday business life for many companies. Lower wages and decreased regulation can make outsourcing seem appealing to companies trying to cut costs while maintaining quality and services. But the economic benefits alone may not be enough to make outsourcing worthwhile for every business.

Cost Differentials
Labor costs in most other countries are lower than in the United States. Employers not only will pay lower wages, but they won't have to pay unemployment tax, Social Security and Medicare taxes, worker's compensation, health insurance and other employment costs associated with domestic workers. The larger the company, the more employees it can outsource and the greater the savings will be. However, companies still incur costs to supervise these employees and to train them. These costs may escalate over time, eliminating some of the difference between U.S. and foreign wages. When University of South Florida researchers studied wages in popular outsourcing countries in 2004, they found that wages for skilled workers in India were rising 15 percent a year. In addition, labor disputes in developing countries can disrupt work and result in losses for employers. Even when products are much cheaper to produce overseas, the cost of shipping products back to the United State can further reduce cost savings.

Quality Control
While companies can set quality standards for work performed by foreign employees, language and cultural barriers, as well as overseas supply chains, can present barriers to quality control. Products made overseas can be flawed because of out-of-date or worn equipment in overseas factories, or substandard raw materials. In 2000, for example, Masterlock had to recall more than 750,000 locks made in China. Worn dies at the Chinese factory produced locks that could be pulled apart without a key.

Public Image
Companies that move jobs overseas can portray themselves as bringing much-needed jobs and aid to impoverished countries. On the other hand, in times of high unemployment in the United States, sending jobs out of the country can hurt a company's public image. Fewer regulations in other countries can make it less expensive for American factories to operate, but environmental damage and labor abuses that make the news can tarnish the image of companies involved there. Consumers have organized boycotts against companies that use child labor or sweatshops to produce clothing and shoes. In response, companies such as Nike, Dell and Gap have established codes of conduct for their suppliers. Such codes can help improve the image of companies that use outsourcing.

Expand Capabilities
Some companies turn to outsourcing because they can't find the skills or equipment they need to produce their product or service here in the United States. Outsourcing production of a new product can allow you to get to market sooner than if you had to build your own factory, acquire equipment and hire employees. Some countries, such as India, offer large pools of high tech workers. If you operate in an area where such workers are scarce, turning to outsourcing could help fill those jobs with competent employees.

10.4.4 Strategies for Successful Offshore Outsourcing:

Successful projects require day-to-day interaction between software development and business teams, so it is essential for the hiring company to take a hands-on approach to project management. Companies cannot afford to outsource responsibility and accountability.

To improve the chances that an offshore outsourcing project will succeed, a company must carefully evaluate whether an outsourcing firm can provide the following:

1. Employees with the required expertise in the technologies involved in the project

2. A project manager who speaks the employer company's native language

3. A pool of staff large enough to meet the needs of the project

4. A state-of-the-art telecommunications setup

5. High-quality on-site managers and supervisors

10.5 WHISTLES-BLOWING:

Q. What is Whistle- blowing and what ethical issue is associated with it? W/13 S/14 W/14 S/15 CSE S/14 IT W/14 IT,
Q. Highlight key issue that a potential whistle blower should consider W/13 IT

‣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 them 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.

‣In going public with the information they have, whistle-blowers often risk their own careers and sometimes even affect the lives of their friends and family.

‣In extreme situations, whistle-blowers must choose between protecting society and remaining silent.

10.5.1 Protection for Whistle-Blowers

‣Whistle-blower protection laws allow employees to alert the proper authorities to employer actions that are unethical, illegal, or unsafe, or that violate specific public policies.

‣Unfortunately, no comprehensive federal law protects all whistle-blowers from retaliatory acts. Instead, numerous laws protect a certain class of specific whistle-blowing acts in various industries.

‣To make things even more complicated, each law has different filing provisions, administrative and judicial remedies, and statutes of limitations (which set time limits for legal action).

‣Thus, the first step in reviewing a whistle-blower's claim of retaliation is for an experienced attorney to analyze the various laws and determine if and how the employee is protected. Once that is known, the attorney can determine what procedures to follow in filing a claim.

‣From the whistle-blower's perspective, a short statute of limitations is a major weakness of many whistle-blower protection laws.

‣ Failure to comply with the statute of limitations is a favorite defense of firms accused of wrongdoing in whistle-blower cases.

10.5.2 Whistle-Blowing Protection for Private-Sector Workers

‣Under state law, an employee could traditionally be terminated for any reason, or no reason, in the absence of an employment contract.

‣However, many states have created laws that prevent workers from being fired because of an employee's participation in"protected"activities.

‣One such activity is the filing of a qui tam lawsuit under the provisions of the False Claims Act.

‣States that recognize the public benefit of such cases offer protection to whistle-blowers; for example, whistle-blowers can file claims against their employers for retaliatory termination and are entitled to jury trials.

‣ If successful, they can receive punitive damage awards.

10.5.3 Dealing with a Whistle-Blowing Situation

‣Each potential whistle-blowing case involves different circumstances, issues, and personalities. Two people working together in the same company may have different values and concerns that cause them to react in different ways to a particular situation—and both reactions might be ethical.

‣It is impossible to outline a definitive step-by-step procedure of how to behave in a whistle-blowing situation.

10.5.4 Assess the Seriousness of the Situation

‣Before considering whistle-blowing, a person should have specific knowledge that his company or a coworker is acting unethically and that the action represents a serious threat to the public interest.

‣The employee should carefully and informally seek trusted resources outside the company and ask for their assessment.

‣Their point of view may help the employee see the situation from a different perspective and alleviate concerns.

‣On the other hand, the outside resources may reinforce the employee's initial suspicions, forcing a series of difficult ethical decisions.

10.5.5 Begin Documentation

‣An employee who identifies an illegal or unethical practice should begin to compile adequate documentation to establish wrongdoing.

‣ The documentation should record all events and facts as well as the employee's insights about the situation.

‣This record helps construct a chronology of events if legal testimony is required in the future.

‣An employee should identify and copy all supporting memos, correspondence, manuals, and other documents before taking the next step.

‣ The employee should maintain documentation and keep it up to date throughout the process.

10.5.6 Attempt to Address the Situation Internally

An employee should next attempt to address the problem internally by providing a written summary to the appropriate managers, including a statement that they either responded or clearly chose not to respond. Ideally, the employee can expose the problem and deal with it from inside the organization. The focus should be on disclosing the facts and how the situation affects others. The employee's goal should be to fix the problem, not to place blame.

10.5.7 Consider Escalating the Situation Within the Company

The employee's initial attempt to deal with a situation internally may be unsuccessful. At this point, the employee may rationalize that he or she has done all that is required by raising the issue. Others may feel so strongly about the situation that they are compelled to take further action. Thus, a determined and conscientious employee may feel forced to choose between escalating the problem and going over the manager's head or going outside the organization to deal with the problem. The employee may feel obligated to sound the alarm on the company because there appears to be no chance to solve the problem internally.

10.6 GREEN COMPUTING

Q. Short note on Green Computing W/13, S/14 CT W/13, S/14, S/15 CSE , CT

‣ 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.

‣ However, to manufacturer a truly green PC, hardware companies must also reduce the amount of hazardous materials used and dramatically increase the amount of reusable or recyclable materials used.

‣ The manufacturers must also help consumers dispose of their products in an environmentally safe manner at the end of their useful life.

‣Electronic devices such as personal computers and cell phones contain hundreds or even thousands of components.

‣ The components, 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, brominates 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.

‣Users of these products can also be exposed to these materials when using poorly designed or improperly manufactured devices.

‣ Care must also be taken when recycling or destroying these devices to avoid contaminating the environment.

‣The United States has no federal law prohibiting the export of toxic waste, so many used electronic devices intended for recycling are sold to companies in developing countries that try to repair the components or extract valuable metals from them, using methods that release carcinogens and other toxins into the air and the water supply.

To promote green computing concepts at all possible levels, the following four complementary approaches are employed:

- **Green use**: Minimizing the electricity consumption of computers and their peripheral devices and using them in an eco-friendly manner
- **Green disposal**: Re-purposing an existing computer or appropriately disposing of, or recycling, unwanted electronic equipment
- **Green design**: Designing energy-efficient computers, servers, printers, projectors and other digital devices
- **Green manufacturing**: Minimizing waste during the manufacturing of computers and other subsystems to reduce the environmental impact of these activities

Government regulatory authorities also actively work to promote green computing concepts by introducing several voluntary programs and regulations for their enforcement.

Average computer users can employ the following general tactics to make their computing usage more green:

- Use the hibernate or sleep mode when away from a computer for extended periods
- Use flat-screen or LCD monitors, instead of conventional cathode ray tube (CRT) monitors
- Buy energy efficient notebook computers, instead of desktop computers

- Activate the power management features for controlling energy consumption
- Make proper arrangements for safe electronic waste disposal
- Turn off computers at the end of each day
- Refill printer cartridges, rather than buying new ones
- Instead of purchasing a new computer, try refurbishing an existing device
-

10.7 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 EICC focuses on the areas of worker safety and fairness, environmental responsibility, and business efficiency. Information and communications technology organizations, electronic manufacturers, software firms, and manufacturing service providers may voluntarily join the coalition.

▪The EICC has established a code of conduct that defines performance, compliance, auditing, and reporting guidelines across five areas of social responsibility: labor, health and safety, environment, management system, and ethics.

▪Adopting organizations apply the code across their entire worldwide supply chain and require their first-tier suppliers to acknowledge and implement it.

▪As of July 2009, the code has been formally adopted by over 38 EICC member organizations, including Adobe, Cisco, Dell, HP, IBM, Intel, Microsoft, Philips, Samsung, and Sony.

The following are the five areas of social responsibility and guiding principles covered by the code:

1. 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

2. **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 ongoing worker input and education is essential to identifying and solving health and safety issues in the workplace."

3. **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."

4. **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."

5. **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.

10.8 Hazardous materials in computers :

Q. Discuss the use of Hazardous materials in computers W/13, W/14 CT

E-Waste Component	Process Used	Potential Environmental Hazard
Cathode ray tubes (used in TVs, computer monitors, ATM, video cameras, and more)	Breaking and removal of yoke, then dumping	Lead, barium and other heavy metals leaching into the ground water and release of toxic phosphor
Printed circuit board (image behind table - a thin plate on which chips and other electronic components are placed)	De-soldering and removal of computer chips; open burning and acid baths to remove final metals after chips are removed.	Air emissions as well as discharge into rivers of glass dust, tin, lead, brominated dioxin, beryllium cadmium, and mercury
Chips and other gold plated components	Chemical stripping using nitric and hydrochloric acid and burning of chips	Hydrocarbons, heavy metals, brominated substances discharged directly into rivers acidifying fish and flora. Tin and lead contamination of surface and groundwater. Air emissions of brominated dioxins, heavy metals and hydrocarbons
Plastics from printers, keyboards, monitors, etc.	Shredding and low temp melting to be reused	Emissions of brominated dioxins, heavy metals and hydrocarbons
Computer wires	Open burning and stripping to remove copper	Hydrocarbon ashes released into air, water and soil.

10.9 Employee Leasing

Q. Short note on Employee Leasing W/13 W/14 CT

▪ *Workers who are officially employed by a professional employer organization, which is responsible for overseeing all HR-related functions, but who actually perform all work for your company* .

▪Employee leasing is a contractual arrangement in which the leasing company, also known as a professional employer organization (PEO), is the official employer.

▪ Employment responsibilities are typically shared between the leasing company and the business owner (you, in this case).

▪You retain essential management control over the work performed by the employees. The leasing company, meanwhile, assumes responsibility for work such as reporting wages and employment taxes.

▪ Your main responsibility is writing a check to the leasing company to cover the payroll, taxes, benefits and administrative fees. The PEO does the rest.

▪Employee leasing lets you add workers without adding administrative complexity.

▪Employee leasing firms manage compliance with state and federal regulations, payroll, unemployment insurance, W-2 forms claims processing, and other paperwork.

▪ Some also offer pension and employee assistance programs.

▪By combining the employees of several companies into one large pool, PEOs can also offer business owners better rates on health-care and workers' compensation coverage. The net effect can be significant savings of your time and money.