

Unit 1 An Overview of Ethics, Ethics or IT Workers and IT users

Contents:

- Ethics, Ethics in Business World
- Corporate Social Responsibility
- Fostering Corporate Social Responsibility and Good Business Ethics
- Improving Business Ethics
- Ethical Considerations in Decision Making
- Ethics in Information Technology
- Managing IT Worker Relationship
- Encouraging Professionalism of IT Workers – Professional codes of Ethics, Professional Organizations, Certifications and Licensing
- Encouraging Ethical Use of IT Resources among Users

Ethics

- Ethics is a code of behavior that is defined by the group to which an individual belongs. Ethical behavior conforms to generally accepted norms, which may change over time to meet the evolving needs of the society or a group of people who share similar laws, traditions, and values that provide structure to enable them to live in an organized manner.
- Ethics is a branch of philosophy that deals with the principles of conduct of an individual or group. It works as a guiding principle as to decide what is good or bad. They are the standards which govern the life of a person. Ethics is also known as moral philosophy. Some ethical principles are:
 - i. Truthfulness
 - ii. Honesty
 - iii. Loyalty
 - iv. Respect
 - v. Fairness
 - vi. Integrity
- At its simplest, ethics is a system of moral principles. They affect how people make decisions and lead their lives.
- Ethics is concerned with what is good for individuals and society and is also described as moral philosophy.
- Ethics help member of a group understand their roles and responsibilities so they can work together to achieve mutual benefits such as security, access to resources, and the pursuit of life goals.

Ethics covers the following problems:

- how to live a good life
- our rights and responsibilities
- the language of right and wrong
- moral decisions - what is good and bad?

Our concepts of ethics have been derived from religions, philosophies and cultures. They infuse debates on topics like abortion, human rights and professional conduct.

Approaches to ethics

Philosophers nowadays tend to divide ethical theories into three areas: **metaethics**, **normative ethics** and **applied ethics**.

- Meta-ethics deals with the nature of moral judgement. It looks at the origins and meaning of ethical principles.
- Normative ethics is concerned with the content of moral judgements and the criteria for what is right or wrong.
- Applied ethics looks at controversial topics like war, animal rights and capital punishment.

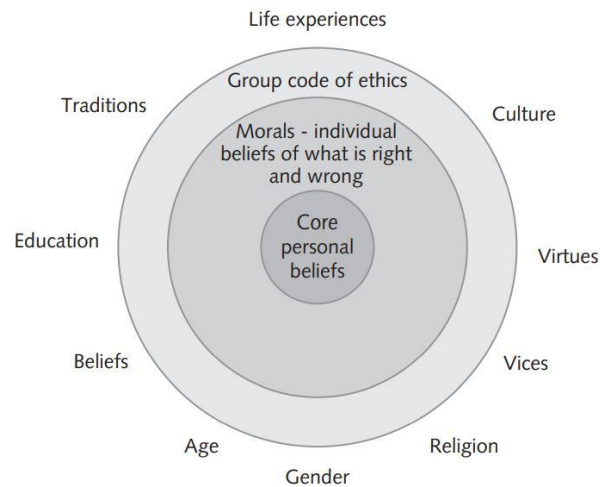
Morals:

- Morals are the social, cultural and religious beliefs or values of an individual or group which tells us what is right or wrong. They are the rules and standards made by the society or culture which is to be followed by us while deciding what is right. Some moral principles are:
 - i. Do not cheat
 - ii. Be loyal
 - iii. Be patient
 - iv. Always tell the truth
 - v. Be generous
- Morals refer to the beliefs what is not objectively right, but what is considered right for any situation, so it can be said that what is morally correct may not be objectively correct.
- Morals are the personal principles upon which an individual bases his or her decisions about what is right and what is wrong. They are the core belief formed and adhered to by an individual.
Example: Many of us have a core belief that all people should be treated with respect and this belief governs our actions towards others.
Your moral principles are statement of what you believe to be rules of right conduct.
- Nearly everyone would agree that certain behaviors – such as lying and cheating – are wrong. However, opinions about what constitutes right and wrong behaviors can vary dramatically.

For example, attitudes towards software piracy range from strong opposition to acceptance of the practice exists. According to the Business Software Alliance (BSA), the global rate of software piracy stands at round 42%. The piracy rate is nearly 80% across the continent of Africa, 63% in Asia, 73% in India and 57% in Nepal. Many consumers simply cannot afford software licenses and pirated copies are readily available at cut-rate prices.

- Individual views of what behavior is moral may be impacted by a person's age, cultural group, ethnic background, religion, life experiences, education, and gender along with many other factors.
- Activities like murder, theft and arson are immoral but other behaviors that are accepted in one culture might not be acceptable to another. Even within the same society, people can have strong disagreements over some moral issues.
For example, in US, issues such as abortion, stem cell research, death penalty, same-sex marriage, marijuana usage, and gun control are continuously debated, and people on both sides of these debates feel that their arguments are on solid moral ground.
- On some occasions, we can encounter situations in which the ethics of the group to which we belong are in conflict with our individual morals.
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 morally objectionable crime.

The relationship between ethics and morals



The major differences between Morals and Ethics are:

1. Morals deal with what is 'right or wrong'. Ethics deals with what is 'good or evil'.
2. The term morals is derived from a Greek word 'mos' which refers to custom and the customs are determined by group of individuals or some authority. On the other hand, ethics is originated from Greek word 'ethikos' which refers to character and character is an attribute.
3. Morals are dictated by society, culture or religion while Ethics are chosen by the person himself which governs his life.
4. Morals are concerned with principles of right and wrong. On the contrary, ethics stresses on right and wrong conduct.
5. As morals are framed and designed by the group, there is no option to think and choose; the individual can either accept or reject. Conversely, the people are free to think and choose the principles of his life in ethics.
6. Morals may vary from society to society and culture to culture. As opposed to Ethics, which remains same regardless of any culture, religion or society.
7. Morals do not have any applicability to business, whereas Ethics is widely applicable in the business known as business ethics.
8. Morals are expressed in the form of statements, but Ethics are not expressed in the form of statements.

Examples

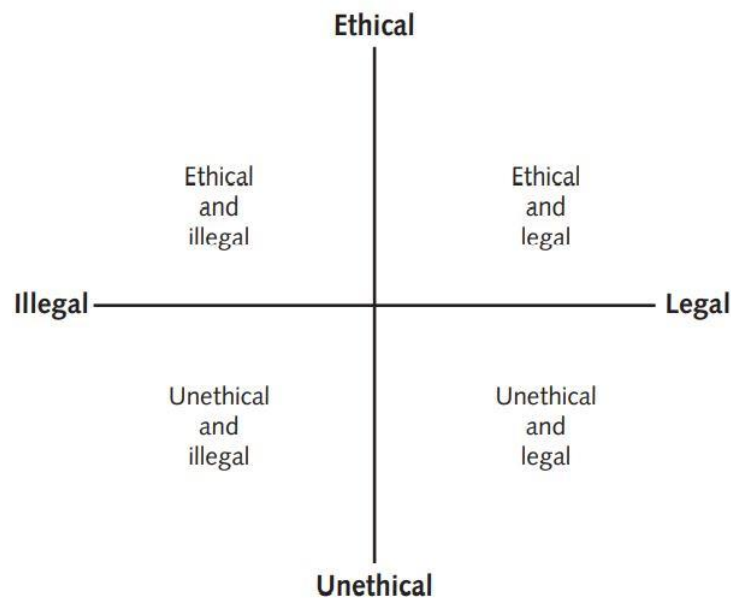
1. If the son of a big politician has committed a crime and he uses his powers to free his son from legal consequences. Then this act is immoral because the politician is trying to save a culprit.
2. A very close friend or relative of an interviewer comes for an interview and without asking a single question, he selects him. This act is unethical because the selection process must be transparent and unbiased.
3. A grocer sells contaminated products to his customers to earn more profit. This act is neither moral nor ethical because he is cheating his customers and profession at the same time.

Law

- Law is a system of rules that tells us what we can and cannot do.
- Laws are enforced by the set of institutions (the police, courts, law-making bodies).
- Violation of law can result in censure, fines, and/or imprisonment.
- Laws in Nepal are made by the various local, state and federal legislatures. Sometimes, the laws of these various jurisdictions are in conflicts, creating confusion and uncertainty.
- Laws are not static, new laws are constantly being introduced and existing laws are repealed (cancelled) or modified.

Comparison between Morals, Ethics and Laws

- Legal acts are acts that conform to the law. Moral acts conform to what an individual believes to be the right thing to do.
- In some cases, like abortion, laws can proclaim as legal, although many people may consider it as immoral.
- In case of using marijuana, laws may proclaim as illegal, although many people can consider this as moral to relieve stress and nausea for people undergoing chemotherapy treatment for cancer.
- Laws raise important and complex issues concerning equality, fairness and justice, but do not provide a complete guide to ethical behavior. Just because an activity is defined as legal doesn't mean that it is ethical.



Ethical but illegal

- 1) When a child is hungry and he stole a loaf of bread from a shop to feed.
- 2) A person violates the traffic rule to rush to the hospital in case of medical emergency.
- 3) It can be illegal not to fulfill a contract, but it might be ethical for any number of logical reasons.
- 4) It is illegal to lease a car or an apartment in your name for someone else who otherwise would not qualify, but it is an ethical thing to do if it is going to help them succeed in life.

Unethical but legal

- 1) Keeping money that someone dropped is legal, but again, many would find it unethical.
- 2) The death penalty is legal in many countries, but large number of individuals consider it unethical.
- 3) Smoking cigarettes in public is legal in some places, but some may find it unethical.
- 4) Abortion is legal in some places, but many consider it as unethical.

Law	Ethics
Law is system of rules governing the whole society and actions of individual members.	Ethics is branch of moral philosophy that helps in guiding people about the conduct of individuals.
Law is set of rules and regulations	Ethics is set of guidelines
Law is pass by a government	Ethics are rules or guidelines set by individuals or legal and professional norms.
Law is expressed and published in writing	Ethics are abstracts
Violation of law leads to punishments like imprisonment or fine or even both.	Violation of ethics does not cause punishment.

Summary: What is ethics?

- Ethics is a code of behavior that is defined by the group to which an individual belongs.
- Morals are the personal principles upon which an individual bases his or her decisions about what is right and what is wrong.
- A person who acts with integrity acts in accordance with a personal code of principles.
- 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, and law-making bodies).
- A code of ethics states the principles and core values that are essential to one's work.
- Just because an activity is defined as legal does not mean that it is ethical.

Ethics in the Business World

- The system of ethical beliefs that guides the values, behaviors, and decisions of a business organization and the individuals within that organization is known as business ethics.
- Some ethical requirements for businesses are codified into law; environmental regulations, the minimum wage, and restrictions against insider trading.
- Ethics has risen to the top of the business agenda because the risks associated with appropriate behavior have increased, both in their likelihood and in their potential negative impact.

For example:

1. The collapse and/or bailout of financial institutions such as Bank of America, CitiGroup, Yes Bank of India due to unwise and/or unethical decision making regarding mortgages, loans, and credit to unqualified individuals and organizations.
2. Numerous corporate officers and senior managers sentenced to prison terms for their unethical behavior. Stewart Parnell, former CEO of Peanut Corporation of America, was sentenced to 28 years in prison for knowingly shipping contaminated food product, resulting nine dead and more than 700 sick.

- Unethical behavior in the business world can lead to serious negative consequences for both organizations and individuals.
- Ethics and moral principles are vital attributes for any business to earn and sustain the trust of customers for longevity, sustain undisputed and unquestioned business for ever, and enjoy long term success in terms of revenue and reputation.
- Many companies having firm ethical and fair trade/business practices are surviving and thriving for centuries, overcoming all upheavals through ages.
- Presence of strong ethical business structure facilitates companies to clearly establish and follow good corporate governance procedures and to foresee and elude any bad business practices.
- Prior to venturing into any line of business or territory, a company must develop a strong business ethical protocol to write off any ethical dilemmas and to handle with any controversial and unprecedented events. Trust, transparency, considerate and reverence are major traits of the business ethics.
- Company have to design their work culture and functionality to develop a trustworthy business and work environment. This is critical to earn the trust of customers, employees, business partners, agents and any third party suppliers.
- Fair, just and equal treatment to all people involved in the business is critical to maintain transparency in:
 - a) Business transaction with customers and external stakeholders; and
 - b) Appraisal system and grievance redress system of the employees.
- Timely consideration and resolution of the customers concerns and real time issues of the employees will be a critical connection in serving customer satisfaction and boosting the morals of the employees.
- Respect towards customers and employees is one of the prime facets in maintaining long term relationship with customers and retaining the qualified and talented employees for long period of time.
- Every business should have a unique and dedicated business ethical protocol and a training system in place to educate the people (internal and external) associated with the business about the criticality of observing the business ethical protocol to conduct the business in ethical and transparent manner.

Features of Business ethics

Business ethics of a company will reflect in its moral, ethical and social values. Such moral, ethical and social values of a company shall comprise of:

- i. Honest service to customers.
- ii. Following statutory approved protocols for customer protection and safety.
- iii. Equal and fair treatment to all the people connected to the business.
- iv. No mental, physical and economic exploitation of any group or person who are serving the business.
- v. Business ethics is a moral responsibility of a company to thrive the business on certain set of moral and ethical values.
- vi. Integration of right set of moral and social values into business structure will protect the business and economic interests of all business stakeholders.
- vii. A standard business ethics protocol will clearly establish business limitations in terms of legal, social, economic, cultural and other limits.
- viii. Educating the business stakeholders about the benefits of observing business ethics protocol and preserving moral and ethical values will define the course of the business in terms of reputation, revenue and durability.
- ix. Despite of size and magnitude of business it is moral responsibility of every company to establish business ethics protocol and to ensure all stakeholders are observing the business ethics protocol without fail.

Some unethical practices devastating the business ethics

Economic and Financial Scandals

- i. Manipulation of financial and business data
- ii. Illegal usage of price sensitive information of business
- iii. Bribery to certain internal and external stakeholders
- iv. Unauthorized related party transactions
- v. Insider trading acts

Intellectual Property Rights (IPR)

- i. Unauthorized usage of IPR of another person/company by a company for its benefit or any third party benefit
- ii. Usage of a product or service in violation or violation of third party IPR
- iii. Exploiting the IPR of a person with unfair terms and conditions in a contract

Professional and Behavioral Matters

- i. Sexual harassment
- ii. Discrimination in job/work allocation to employees
- iii. Negligence in handling the safety and health of the professionals
- iv. Exploiting the talent of professionals with payment of unfair compensation
- v. Events impacting privacy of the professionals and business stakeholders
- vi. Unfair terms and conditions of the employment agreement
- vii. Efforts to dismantle the union of the professionals

Marketing Aspects

- i. Circulation of marketing content which is against public policy and moral values of the society
- ii. Misleading advertisements
- iii. Circulation of marketing content with prime focus on business and revenue generation by any means rather than serving the requirements and interests of the clients
- iv. Usage of unethical methods in marketing to target specific category of consumers
- v. Deceptive marketing strategies.

History has proven from time to time that companies which craved for short term success by resorting to unethical and unfair trade practices have crumbled to ground from top position following the unveiling of the fraud which was basis for such short term success.

To avoid the aforesaid fate, establishing and observing standard business ethics is moral responsibility of every company and is also only way out for companies to sustain long term success, to retain the customer base for longevity and to reign as market leaders in their line of business.

Examples of lapses in business ethics by employees in IT organization

1. Volkswagen has admitted that 11 million of its vehicles were equipped with software that was used to cheat on emissions test. The company is now contending with the consequence.
2. Toshiba, the Japanese industrial giant whose diversified products and services include IT and communication equipment and systems, disclosed that it overstated its earnings over a seven-year period by more than \$1.2 billion.

3. Amazon has the second highest employee turnover rate of companies in the Fortune 500 and has been criticized by some for creating a high pressure work environment in which bosses' expectations were almost impossible to satisfy and jobs were threatened if illness or other personal issues influenced on work.

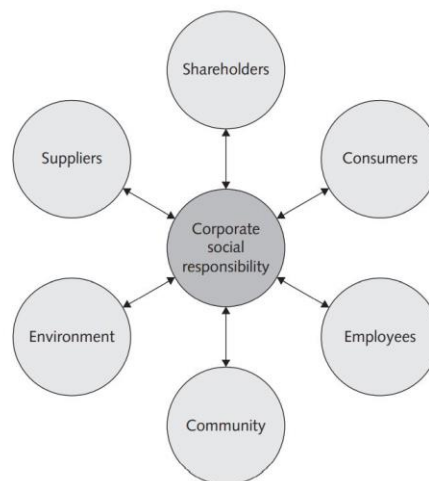
Suppose, you are hired at a large software company and have been working overtime for the last two months trying to complete the final testing of a new software release for the company's flagship product, which is used by thousands of organizations worldwide. Unfortunately, the software has many bugs and testing has taken weeks longer than expected. This afternoon your boss asked you to sign off on the completion of your portion of testing. He explains that the project has gone over budget and is in danger of missing the committed release date for customers. When you object because you feel the software is still buggy, he says not to worry, whatever bugs remain will be fixed in the next release of the software. What do you do?

Summary: What trends have increased the likelihood of an unethical behavior?

- Globalization has created a much more complex work environment, making it more difficult to apply principles and codes of ethics consistently.
- Organizations may be tempted to resort to unethical behavior to maintain profits in today's more challenging and uncertain economic climate.
- It is not unusual for powerful, highly successful individuals to fail to act in morally appropriate ways as such people are often aggressive in striving for what they want and are used to having privileged access to information, people, and other resources. Furthermore, their success often inflates their belief that they have the ability and the right to manipulate the outcome of any situation.

Corporate Social Responsibility (CSR)

- CSR is the concept that an organization should act ethically by taking responsibility for the impact of its actions on its shareholders, consumers, employees, community, environment, and suppliers.



- An organization's approach to CSR can encompass a wide variety of tactics such as:
 - i. Donating a portion of net profit to charity.
 - ii. Implementing more sustainable business operations.
 - iii. Encouraging employee education through tuition fee reimbursement.
 - iv. Supporting environment conservation programs.
- Categories of CSR: Although corporate social responsibility is a very broad concept that is understood and implemented differently by each firm, the underlying idea of CSR is to operate in an economically, socially, and environmentally sustainable manner.

Generally, corporate social responsibility initiatives are categorized as follows:

- i. **Environmental responsibility:** This initiatives aim at reducing pollution and greenhouse gas emissions, and the sustainable use of natural resources.
 - ii. **Human rights responsibility:** This initiatives involve providing fair labor practices (e.g., equal pay for equal work) and fair trade practices, and disavowing child labor.
 - iii. **Philanthropic responsibility:** It includes things such as funding educational programs, supporting health initiatives, donating to causes, and supporting community beautification projects.
 - iv. **Economic responsibility:** This initiatives involve improving the firm's business operation while participating in sustainable practices – for example, using a new manufacturing process to minimize wastage.
- Setting CSR goals encourages an organization to achieve higher moral and ethical standards.
 - Supply chain sustainability is a component of CSR that focuses on developing and maintaining a supply chain that meets the needs of the present without compromising the ability of future generations to meet their needs. It takes into account issues such as fair labor practices, energy, and resource conservation, human rights, and community responsibility. Many IT equipment manufacturers have made supply chain sustainability a priority as they must comply various directives and regulations. In many cases, meeting supply chain sustainability goals can also lead to lower costs.
- For example, in fiscal year 2015, Dell launched its closed-loop plastics supply chain and by year end had recycled 2.2 million pounds of those plastics back into new Dell products. In addition, its global takeback program has made Dell the world's largest technology recycler, collecting more than 1.4 billion pounds of e-waste since 2007.
- Each organization must decide if CSR is a priority and, if so what its specific CSR goals are?
 - The pursuit of some CSR goals can lead to increased profits, making it easy for senior management and stakeholders to support the organization's goals. However, if attempt to meet specific CSR goal leads to a decrease in profits, senior management may be challenged to modify or drop the CSR goal entirely.
 - Many organizations define a wide range of corporate responsibility areas that are important to them, their customers, and their community. In order for a CSR program to be effective, a senior executive should be placed in charge of corporate responsibility results for each area, with strategic initiatives defined, staffed and well-funded. Key indicators of progress in these areas should be define and the results tracked and reported to measure progress.

TABLE 1-2 Intel Corporate Responsibility Report for 2015

Key performance area	Key performance indicator	2015 value
Financial results and economic impact	Net revenue	\$55.4B
	Net income	\$11.4B
	Provision for taxes	\$2.8B
	Research and development spending	\$12.1B
	Capital investments	\$7.3B
	Customer survey “Delighted” score	87%
Environmental sustainability	Greenhouse gas emissions (millions of metric tons of CO ₂)	2.00
	Energy usage (billions of kWh)	6.4
	Total water withdrawn (billions of gallons)	9.0
	Hazardous waste generated (thousands of tons)/% to landfill	61.6/2
	Nonhazardous waste generated (thousands of tons)/% recycled	80.8/82
Our people	Employees at year end (thousands)	107.3
	Women in global workforce (percent)	25%
	Women on our board of directors at year-end (percent)	18%
	Investment in training (millions of dollars)	\$278
	Safety (recordable rate/days away case rate)	0.58/0.11
	Organizational Health Survey scores—“Proud to Work for Intel”	84% (2014)
Social impact	Employee volunteerism rate	41%
	Worldwide charitable giving (dollars in millions)	\$90.3
	Charitable giving as a percentage of pre-tax net income	0.6%
Supply chain responsibility	Supplier audits (third-party and Intel-led audits)	121

Business Benefits of CSR

In a way, CSR can be seen as a public relations effort. However, it goes beyond that, as CSR can also boost a firm’s competitiveness. The business benefits of CSR include the following:

- i. **Stronger brand image, recognition, and reputation:** CSR adds value to firms by establishing and maintaining a good corporate reputation and/or brand equity.
- ii. **Increased customer loyalty and sales:** Customers of a firm that practices CSR feel that they are helping the firm support good causes.
- iii. **Operational cost savings:** Investing in operational efficiencies results in operational cost savings as well as reduced environmental impact.
- iv. **Retaining key and talented employees:** Employees often stay longer and are more committed to their firm knowing that they are working for a business that practices CSR.
- v. **Easier access to funding:** Many investors are more willing to support a business that practices CSR.
- vi. **Reduced regulatory burden:** Strong relationships with regulatory bodies can help to reduce a firm’s regulatory burden.

Fostering (Promoting) Corporate Social Responsibility and Good Business Ethics

Organizations have at least five good reasons to pursue CSR goals and to promote a work environment in which employees are encouraged to act ethically when making business decisions:

1. Gaining the goodwill 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

Gaining the goodwill of the community:

- Although organizations exist primarily to earn profits or provide services to customers, they also have some fundamental responsibilities to society.
- All successful organizations, including technology firms, recognize that they must attract and maintain loyal customers. Philanthropy is one way in which an organization can demonstrate its values in action and make a positive connection with its stakeholders.
- As a result, many organizations initiate or support socially responsible activities, which may 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.

Examples:

1. Dell Inc. has several initiatives aimed at reducing the amount of natural resources it takes to create and ship its products, cutting the amount of energy it takes its customers to use its products, and curbing the effects its products have on people and the planet.
2. Google agreed to invest more than \$1.5 billion in renewable energy projects, such as large-scale wind farms and rooftop solar panels.
3. IBM created a program to train transitioning service members to become certified as advanced data analysts. The company also launched the P-TECH program to help students from low-income families finish high school and obtain associate degrees. Several graduates of the program have taken entry level jobs at IBM while continuing to work toward a four-year degree.
4. Microsoft made \$922 million in technology donations to more than 120,000 nonprofit organizations globally, and its employees contributed \$117 million to 20,000 nonprofits through the company's corporate giving program.
5. Oracle delivered nearly \$5 billion in resources (with a focus on computer science education) to help 2.2 million students in 100 countries become college-and-career ready.

- The goodwill that CSR activities generate can make it easier for corporations to conduct their business. For example, a company known for treating its employees well will find it easier to compete for the top job candidates.

Creating an organization that operates consistently:

- Organizations develop and abide 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 a consistency ensures 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:
 - i. Operate with honesty and integrity, staying true to organizational principles
 - ii. Operate according to standards of ethical conduct, in words and action
 - iii. Treat colleagues, customers, and consumers with respect
 - iv. Strive to be the best at what matters most to the organization
 - v. Value diversity
 - vi. Make decisions based on facts and principles

Fostering good business practices:

- In many cases, good ethics can mean good business and improved profits.
 - i. Companies that produce safe and effective products avoid costly recalls and lawsuits.
 - ii. Companies that provide excellent service retain their customers instead of losing them to competitors.
 - iii. Companies that develop and maintain strong employee relations enjoy lower turnover rates and better employee morale.
 - iv. Suppliers and other business partners often place a priority on working with companies that operate in a fair and ethical manner.
- All these factors tend to increase revenue and profits while decreasing expenses. As a result, ethical companies tend to be more profitable over the long term than unethical companies.
- On the other hand, bad ethics can lead to bad business results. Bad ethics can have a negative impact on employees, many of whom may 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.

Protecting the organization and its employees from legal action:

- In a 1909 ruling the U.S. Supreme Court established that an employer can be held responsible for the acts of its employees even if the employees act in a manner contrary to corporate policy and their employer's directions. The principle established is called respondeat superior, or "let the master answer."
- When it was uncovered that employees of Wells Fargo Bank opened over 2 million bogus credit card accounts not authorized by its customers, the bank was fined over \$185 million and ordered to pay customers full restitution for any fees or charges they may have incurred. The practice began at least as early as 2011 and was an attempt by thousands of bank employees to achieve their sales targets for cross-selling and be rewarded with higher sales bonuses. Cross-selling is the practice of selling multiple products to the existing customers—savings account, checking account, auto loan, mortgage, credit card, etc. Cross-selling to existing customers is cheaper than locating and selling to brand new customers. It also tends to lock existing customers into your bank.
- 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. However, some people argue that officers of companies should not be given light sentences if their ethics programs fail to deter criminal activity within their firms.

Avoiding unfavorable publicity:

- The public reputation of a company strongly influences 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.

- Prominent ad buyers and marketers are angry with Facebook after finding out that the world's largest online social network service greatly exaggerated the average viewing time of video ads on its platform. This is a key metric used by advertisers in deciding how much to spend on Facebook video versus other video services such as YouTube, Twitter, and TV networks. It turns out that Facebook was not including views of three seconds or less in calculating its average view time, resulting in overestimating viewing time by 60 to 80 percent. Some advertising industry analysts believe that the new viewing time results and bad publicity associated with the incident will be impactful in the future placement of tens of billions of advertising dollars.

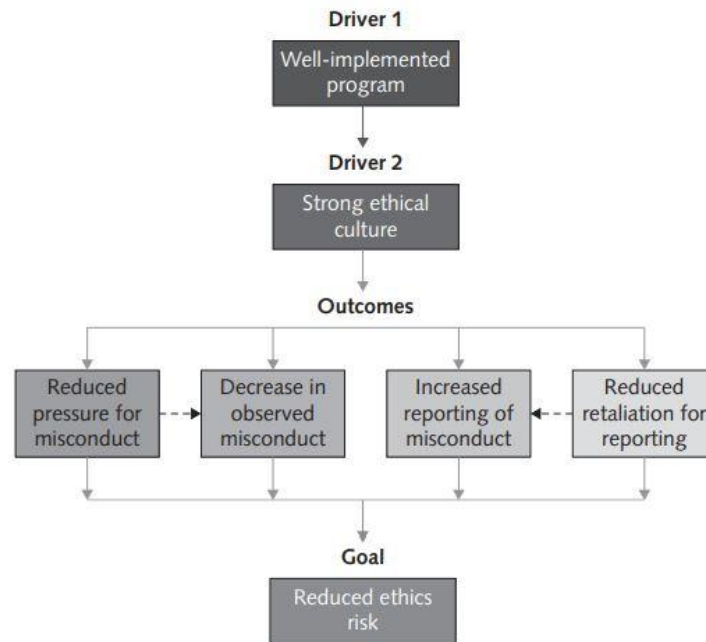
Summary: What is corporate social responsibility, and why is fostering good business ethics important?

- Corporate social responsibility is the concept that an organization should act ethically by taking responsibility for the impact of its actions on its shareholders, consumers, employees, community, environment, and suppliers.
- Supply chain sustainability is a component of CSR that focuses on developing and maintaining a supply chain that meets the needs of the present without compromising the ability of future generations to meet their needs.
- Each organization must decide if CSR is a priority, and if so, what its specific CSR goals are.
- Organizations have five good reasons for pursuing CSR goals and promoting a work environment in which they encourage employees to act ethically:
 - (1) to gain the goodwill of the community,
 - (2) to create an organization that operates consistently,
 - (3) to foster good business practices,
 - (4) to protect the organization and its employees from legal action, and
 - (5) to avoid unfavorable publicity.

Improving Business Ethics

Research by the Ethics Resource Center (ERC) found that 86 percent of the employees in companies with a well-implemented ethics and compliance program are likely to perceive a strong ethical culture within the company, while less than 25 percent of employees in companies with little to no program are likely to perceive a culture that promotes integrity in the workplace.

- A well-implemented ethics and compliance program and a strong ethical culture can, in turn, lead to less pressure on employees to misbehave and a decrease in observed misconduct.
- It also creates an environment in which employees are more comfortable reporting instances of misconduct, partly because there is less fear of potential retaliation by management against reporters (for example, reduced hours, transfer to less desirable jobs, and delays in promotions).
- The Ethics Resource Center has defined the following characteristics of a successful ethics program:
 - i. Employees are willing to seek advice about ethics-related issues.
 - ii. Employees feel prepared to handle situations that could lead to misconduct.
 - iii. Employees are rewarded for ethical behavior.
 - iv. The organization does not reward success obtained through questionable means.
 - v. Employees feel positively about their company.



Some of the actions corporations can take to improve business ethics:

- i. **Appoint 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. This individual “aligns the practices of a workplace with the stated ethics and beliefs of that workplace, holding people accountable to ethical standards”.
- ii. **Require the Board of Directors to Set and Model High Ethical Standards:** The board of directors is responsible for the careful and responsible management of an organization. Board members are expected to conduct themselves according to the highest standards for personal and professional integrity while setting the standard for companywide ethical conduct and ensuring compliance with laws and regulations.
- iii. **Establish a Corporate Code of Ethics:** A code of ethics is a statement that highlights an organization’s key ethical issues and identifies the primary values and principles that are important to the organization and its decision making. Codes of ethics frequently include a set of formal, written statements about the purpose of an organization, its values, and the principles that should guide its employees’ actions.

Intel Code of Conduct Principles

The code affirms Intel’s five principles of conduct:

1. Conduct business with honesty and integrity.
2. Follow the letter and spirit of the law.
3. Treat each other fairly.
4. Act in the best interests of Intel and avoid conflicts of interest.
5. Protect the company’s assets and reputation

- iv. **Conduct Social Audits:** In a social audit, an organization reviews how well it is meeting its ethical and social responsibility goals and communicates its new goals for the upcoming year. This information is shared with employees, shareholders, investors, market analysts, customers, suppliers, government agencies, and the communities in which the organization operates.
- v. **Require Employees to Take Ethics Training:** Organization’s code of ethics must be promoted and continually communicated within the organization, from the top to the bottom. Organizations can

do this by showing the 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.

- vi. **Include Ethical Criteria in Employee Appraisals:** Managers can help employees to meet performance expectations by monitoring employee behavior and providing feedback; increasingly, managers are including ethical conduct as part of an employee's performance appraisal.
- vii. **Create an Ethical Work Environment:** Most employees want to perform their jobs successfully and ethically, but good employees sometimes make bad ethical choices. Employees in highly competitive workplaces often feel pressure from aggressive competitors, cutthroat suppliers, unrealistic budgets, unforgiving quotas, tight deadlines, and bonus incentives. Employees may also be encouraged to do "whatever it takes" to get the job done. In such environments, some employees may feel pressure to engage in unethical conduct to meet management's expectations, especially if the organization has no corporate code of ethics and no strong examples of senior management practicing ethical behavior.

Employees must have a knowledgeable resource with whom they can discuss perceived unethical practices.

For example, Intel expects employees to report suspected violations of its code of conduct to a manager, the Legal or Internal Audit Departments, or a business unit's legal counsel. Employees can also report violations anonymously through an internal website dedicated to ethics. Senior management at Intel has made it clear that any employee can report suspected violations of corporate business principles without fear of reprisal or retaliation.

Summary: What measures can organizations take to improve their business ethics?

An organization can take several actions to improve its business ethics including:

- appointing a corporate ethics officer,
- requiring its board of directors to set and model high ethical standards, establish a corporate code of ethics,
- conduct social audits,
- require employees to take ethics training,
- include ethical criteria in employee appraisals, and
- create an ethical work environment.

Ethical Considerations in Decision Making

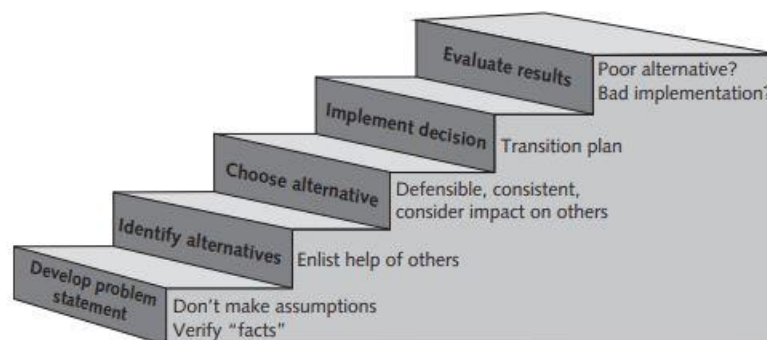


Figure: 5-step ethical decision making process

Steps involved in ethical decision making process are:

1. Develop problem statements
2. Identify alternatives
3. Choose alternatives
4. Implement decision
5. Evaluate results

Develop problem statements:

A problem statement is a clear, concise 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 anyone else affected?
- How often does the problem 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. We must gather and analyze facts, seek information and opinions from the variety of people to develop a good problem statement.

Examples:

1. Good problem statement: Our product supply organization is continually running out of stock of finished products, creating an out-of-stock situation on over 15% of our customer orders, resulting the loss of sales over \$300,000 per month.
2. Poor problem statement: We need to implement a new inventory control system (This is a possible solution, not the problem statement).
3. Poor problem statement: We need to install cameras and monitoring equipment to put an end to theft of finished product in the warehouse (This is again the possible solution, not the problem statement. Are there enough evidence/fact to support that the theft has occurred).

Identify alternatives:

During the decision making process, it is better to enlist all the possible alternatives (solutions). Brainstorming, discussion with the stakeholders can help to enlist them.

During any brainstorming process, try not be critical of ideas, as any negative criticism will tend to shut down the discussion, and the flow of ideas will dry up.

Choose alternatives:

Once a set of alternatives has been identified, the group must evaluate them based on numerous criteria, such as:

- Effectiveness of addressing the issue
- The extent of risk associated with each alternative,
- Cost and time to implement

As part of the evaluation process, weigh various laws, guidelines, and principles that may apply. Consider the likely consequences of each alternative from several prospective.

The alternative selected should be:

- Ethically and legally defensible to a collection of your coworkers, peers, and your profession's governing body of ethics,
- Consistent with the organization's policies and code of ethics.
- Take into account the impact on others.
- Provide a good solution to the problem.

Implement the decision:

Once an alternative is selected, it should be implemented in an effective, efficient and timely manner. This is often much easier said than done, because people tend to resist change. Communication is the key to help people accept a change.

A transition plan must be defined to explain to people how they will move from the old way of doing things in new way. The transition should be easy and pain free. It may be necessary to train the people affected, provide incentives for making the change in a successful fashion, and modify the reward system to encourage new behaviors consistent with the change.

Evaluate 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. Were the success criteria fully met? Were there any unintended consequences? This evaluation may indicate that further refinements are needed. If so, return to the problem development step, refine the problem statement as necessary, and work through the process again.

On the other hand, the proper alternative may have been selected, but it was implemented in a poor fashion so the desired results were not achieved. This may require redoing some of the implementation steps.

Summary: How can you include ethical considerations in your decision making?

Often, people employ a simple decision-making model that includes these steps:

- (1) define the problem,
- (2) identify alternatives,
- (3) choose an alternative,
- (4) implement the decision, and
- (5) monitor the results.

You can incorporate ethical considerations into decision making by identifying and involving the stakeholders; weighing various laws, guidelines, and principles—including the organization's code of ethics—that may apply; and considering the impact of the decision on you, your organization, stakeholders, your customers and suppliers, and the environment.

Ethics in Information Technology (IT)

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

In the focus 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:

- Governments around the world have implemented various systems that enable the surveillance of their citizens and are struggling to achieve the proper balance between privacy and security.
- Many employees have their email 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 unwanted email and text messages in an extremely low cost, but intrusive marketing approach.
- Hackers break into databases of financial and retail institutions to steal customer information and then use it to commit identity theft—opening new accounts and charging purchases to unsuspecting victims.
- Students around the world have been caught downloading material from the web and plagiarizing content for their term papers.
- Websites plant cookies or spyware on visitors' hard drives to track their online purchases and activities.

Ethics in IT has two aspects:

- The general public needs to develop a better understanding of the critical importance of ethics as it applies to IT; currently, too much emphasis is placed on technical issues. IT has a deep effect on society, and IT professionals and end users need to recognize this fact when they implement technology and formulate policies that will have legal consequences and affect the wellbeing of millions of consumers.
- Important business-technology decisions with strong ethical implications are too often left to the technical experts to decide (for example, what data to gather about customers, where to store it, how to use it, and what level of security to employ to protect it). General business managers must assume greater responsibility for such decisions, but to do so they must be able to make broad-minded, objective decisions based on technical knowledge, business know-how, and high ethical standards. They must also try to create a working environment in which ethical dilemmas can be discussed openly, objectively, and constructively.

The goals of Ethics in IT are:

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

Summary: What trends have increased the risk that information technology will be used in an unethical manner?

The growth of the Internet and social networks; the ability to capture, store, and analyze vast amounts of personal data; and a 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.

Managing IT Worker relationship

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

These various relationships are discussed below:

1. Relationships between IT Workers and Employers

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

- An IT worker and an employer typically agree on the fundamental aspects of this relationship before the worker accepts an employment offer. These issues may include job title, general performance expectations, specific work responsibilities, dress code, location of employment, salary, work hours, and company benefits.
- Many other aspects of this relationship may be addressed in a company's policy and procedures manual or in the company's code of conduct, if one exists. Topics addressed in such a manual or code of conduct might include protection of company secrets; vacation policy; time off allowed for a funeral or an illness in the family; tuition reimbursement; and use of company resources, including computers and networks.
- 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 issues 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.

As the stewards of an organization's IT resources, IT workers must set an example and enforce policies regarding the ethical use of IT.

IT workers often have the skills and knowledge to abuse systems and data or to enable others to do so. Software piracy is an area in which IT workers may be tempted to violate laws and policies. Although end users often get the blame when it comes to using illegal copies of commercial software, software piracy in a corporate setting is sometimes directly traceable to IT staff members—either they allow it to happen or they actively engage in it, often to reduce IT-related spending.

The Software & Information Industry Association (SIIA) and the BSA | The Software Alliance (BSA) are trade groups that represent the world's largest software and hardware manufacturers. Part of their mission is to stop the unauthorized copying of software produced by its members. North America has the lowest regional rate of software piracy at 17 percent, which represents a commercial value of \$10 billion in lost revenue for software development companies. The global software theft rate for personal computer software is around 43 percent, which equates to a commercial value of \$62.7 billion.

SIIA promotes the common interests of the software and digital content industry. It protects the intellectual property of member companies and advocates a legal and regulatory environment that benefits the entire industry.

BSA membership includes about two dozen global members such as Adobe, Apple, Dell, IBM, Intuit, Microsoft, Oracle, and SAS Institute. In 2012 alone, BSA investigated over 15,000 reports of unlicensed software use around the globe.

Shortly after its one IT staff member left the company, a Texas automotive repair company received a letter from the BSA accusing it of using unlicensed copies of Microsoft software. The company was threatened with a multimillion-dollar fine, one it could not pay and that would force it out of business. To stave off bankruptcy, the company froze salaries and put off the purchase of needed equipment. The dispute was eventually settled for a fraction of the initial amount after the company sought out legal counsel.

Trade secrecy is another area that can present challenges for IT workers and their employers. A trade secret is information, generally unknown to the public, that a company has taken strong measures to keep confidential. It represents something of economic value that has required effort or cost to develop and that has some degree of uniqueness or novelty.

Trade secrets can include the design of new software code, hardware designs, business plans, the design of a user interface to a computer program, and manufacturing processes.

Examples include the Colonel's secret recipe of 11 herbs and spices used to make the original KFC chicken, the formula for Coke, and Intel's manufacturing process for the Core i7-6950K 10-core processing chip.

Employers worry that employees may reveal these secrets to competitors, especially if they leave the company. As a result, companies often require employees to sign confidentiality agreements and promise not to reveal the company's trade secrets.

Another issue that can create friction between employers and IT workers is **whistleblowing**. Whistle-blowing is an effort by an employee to attract attention to a negligent, illegal, unethical, abusive, or dangerous act by a company that threatens the public interest. Whistle-blowers often have special information based on their expertise or position within the offending organization.

For example, an employee of a computer chip manufacturing company may know that the chemical process used to make the chips is dangerous to employees and the general public. A conscientious employee would call the problem to management's attention and try to correct it by working with appropriate resources within the company. But what if the employee's attempt to correct the problem through internal channels was thwarted or ignored? The employee might then consider becoming a whistle-blower and reporting the problem to people outside the company, including state or federal agencies that have jurisdiction. Obviously, such actions could have negative consequences on the employee's job, perhaps resulting in retaliation and firing.

Amazon, IBM, Microsoft, Oracle, and SAP, along with many other companies, are competing in the rapidly growing cloud services arena. Competition is fierce, and the companies all have an incentive to make their cloud services appear financially successful. However, a whistle-blower lawsuit recently filed against Oracle highlighted potential issues related to the way such companies account for income from subscription-based software services that run in the cloud. The whistle-blower, a former Oracle employee, accused management of pressuring her to add millions of dollars in additions to financial reports for expected cloud-based software and services revenue. Accounting experts acknowledge that classifying software sales as cloud or traditional is complex and requires determinations that might subsequently be challenged by auditors. Nonetheless, Oracle shares dropped 4 percent the day following announcement of the lawsuit. Although Oracle alleges the whistle-blower was fired for poor performance, the employee maintains that she was let go just two months after she received a positive job performance review and just one month after the alleged incident began. Oracle strongly denies any allegations of wrong doing and has vowed to countersue the whistle-blower for malicious prosecution.

2. Relationships between IT Workers and Clients

IT workers provide services to clients; sometimes those “clients” are coworkers who are part of the same company as the IT worker. In other cases, the client is part of a different company.

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 a 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 the client and the 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. Such a situation has the potential to undermine the objectivity of an IT worker due to a conflict of interest—a conflict between the IT worker’s (or the IT firm’s) self-interest and the client’s interests.

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 would raise questions about the vendor’s objectivity and the trustworthiness of its recommendations.

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 such a situation, the client may not be informed about a 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 described next.

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

Misrepresentation is the misstatement or incomplete statement of a material fact. If the misrepresentation causes the other party to enter into a contract, that party may have the legal right to cancel the contract or seek reimbursement for damages.

Breach of contract occurs when one party fails to meet the terms of a contract. Further, a material breach of contract occurs when a party fails to perform certain express or implied obligations, which impairs or destroys the essence of the contract. Because there is no clear line between a minor breach and a material breach, determination is made on a case-by-case basis. “When there has been a material breach of contract, the non-breaching party can either:

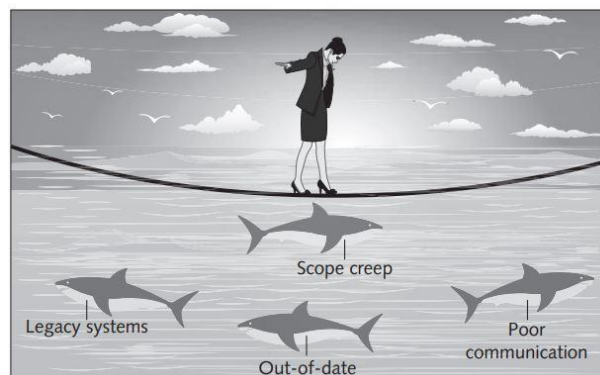
- Withdraw the contract, seek restitution of any compensation paid under the contract to the breaching party, and be discharged from any further performance under the contract; or
- Treat the contract as being in effect and charge the breaching party to recover damages.

In 2016, Hewlett-Packard Enterprise (HPE) was awarded \$3 billion in damages from Oracle after a court determined that Oracle had breached its contract with HPE by dropping support for all Oracle database software being run on HP systems using Intel’s Itanium processor chip. HPE argued that Oracle’s actions dramatically reduced the sale of HPE’s Itanium-based products. HPE also alleged that Oracle’s actions were intended to boost sales of Oracle’s own Sun hardware. The jury ultimately agreed with HPE and awarded it the full amount it was seeking, compensating the company for both lost sales and damages, as well as requiring Oracle to continue supporting Itanium based systems.

When IT projects go wrong because of cost overruns, schedule slippage, lack of system functionality, and so on, upset parties might charge fraud, fraudulent misrepresentation, and/or breach of contract. Trials can take years to settle, generate substantial legal fees, and create bad publicity for both parties. As a result, the vast majority of such disputes are settled out of court, and the proceedings and outcomes are concealed from the public.

In addition, IT vendors have become more careful about protecting themselves from major legal losses by requiring that contracts place a limit on potential damages. Most IT projects are joint efforts in which vendors and customers work together to develop a system. Assigning fault when such projects go wrong can be difficult; one side might be partially at fault, while the other side is mostly at fault. Clients and vendors often disagree about who is to blame in such circumstances.

Frequent causes of problems in IT projects include the following:



- **Scope creep**—Changes to the scope of the project or the system requirements can result in cost overruns, missed deadlines, and a project that fails to meet end-user expectations.

- **Poor communication**—Miscommunication or a lack of communication between customer and vendor can lead to a system whose performance does not meet expectations.
- **Delivery of an obsolete solution**—The vendor delivers a system that meets customer requirements, but a competitor comes out with a system that offers more advanced and useful features.
- **Legacy systems**—If a customer fails to reveal information about legacy systems or databases that must connect with the new hardware or software at the start of a project, implementation can become extremely difficult.

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 can 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 build a good 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 when 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 is the act of providing money, property, or favors to someone in business or government in order 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 a crime if he or she accepts the bribe. 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.

Foxconn Technology, the world's largest electronics contract manufacturer, is headquartered in New Taipei City, Taiwan. The company assembles products for top international brands such as Apple, Nokia, and Sony, and it procures supplies for those products from a wide range of suppliers. In 2014, five former Foxconn employees, including two former senior managers, were charged with bribery for accepting kickbacks from 10 suppliers in exchange for purchasing contracts and assistance clearing Foxconn's quality control checks. Foxconn officials detected the problem and alerted authorities in both Taiwan and China following an internal audit.

In some countries, gifts are an essential part of doing business. In fact, in some countries, it would be considered rude not to bring a present to an initial business meeting. In the United States, a gift might take the form of free tickets to a sporting event from a personnel agency that wants to get on your company's list of preferred suppliers. But, at what point does a gift become a bribe, and who decides?

The key distinguishing factor is that no gift should be hidden. A gift may be considered a bribe if it is not declared. As a result, most companies require that all gifts be declared and that everything but token gifts be declined.

Some companies have a policy of pooling the gifts received by their employees, auctioning them off, and giving the proceeds to charity.

When it comes to distinguishing between bribes and gifts, the perceptions of the donor and the recipient can differ. The recipient may believe he received a gift that in no way obligates him to the donor, particularly if the gift was not cash. The donor's intentions, however, might be very different.

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

4. Relationships between IT Workers and Other Professionals

Professionals often feel a degree of loyalty to the other members of their profession. As a result, they are often quick to help each other obtain new positions but slow to criticize each other in public. 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 by, for example, 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. Many employers consider lying on a résumé as grounds for immediate dismissal.

For instance, Yahoo hired Scott Thompson, the president of eBay's PayPal electronic payments unit, as its new CEO in January 2012; however, Thompson resigned less than a year later over differences in his academic record summarized on his résumé.

Some studies have shown that around 30 percent of all U.S. job applicants exaggerate their accomplishments, while roughly 10 percent "seriously misrepresent" their backgrounds.

Another ethical issue that can arise in relationships between IT workers and other professionals is the inappropriate sharing of corporate information. Because of their roles, IT workers may have access to corporate databases of private and confidential information about employees, customers, suppliers, new product plans, promotions, budgets, and so on. It might be sold to other organizations or shared informally during work conversations with others who have no need to know. Revealing such private or confidential information is grounds for termination in many organizations and could even lead to criminal charges.

5. Relationships between IT Workers and IT Users

The term IT user refers to a person who uses a hardware or software product; the term distinguishes end users 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. They also have a key responsibility to establish an environment that supports ethical behaviors by users. Such an environment discourages software piracy, minimizes the inappropriate use of corporate computing resources, and avoids the inappropriate sharing of information.

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 cannot safeguard against all negative side effects of a product or process. Often, professionals can clearly see the 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.

Clearly, 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 people who live near the plant at risk. As a result, IT workers have a relationship with members of society who may be affected by their actions. There is currently no single, formal organization of IT workers that takes responsibility for establishing and maintaining standards that protect the public.

Take Decision:

You are leading your organization's effort to purchase and install new accounting software. The project will cost an estimated \$3 million, and over the past few months, you have had meetings with several potential vendors to evaluate their offerings and capabilities. It is early March, and the National Collegiate Athletic Association (NCAA) basketball tournament is underway. You receive a phone call from one of the sales reps you met with recently. He has two tickets to the second round games next weekend and wants to give them to you. Can you accept this offer without raising any concerns? How can you turn down this offer without offending the sales rep? Would accepting the offer from the sales rep obligate you in any way? Would you feel compelled to share information with him about where his firm stands in the competition for your business? Would you provide him with any insights about how his firm could make its bid more attractive? Would you be more inclined to spend additional time interacting with him to better understand his firm's products and services?

Summary:

What relationships must an IT worker manage, and what key ethical issues can arise in each?

- An IT worker must maintain good working relationships with employers, clients, suppliers, other professionals, IT users, and society at large. Each relationship has its own set of ethical issues and potential problems.\
- In relationships between IT workers and employers, important issues include setting and enforcing policies regarding the ethical use of IT, the potential for whistle-blowing, and the safeguarding of trade secrets.
- In relationships between IT workers and clients, key issues revolve around defining, sharing, and fulfilling each party's responsibilities for successfully completing an IT project. The IT worker must remain objective and guard against any sort of conflict of interest, fraud, misrepresentation, or breach of contract.
- A major goal for IT workers and suppliers is to develop good working relationships in which no action can be perceived as unethical.

- Bribery is the act of providing money, property, or favors to someone in business or government in order to obtain a business advantage.
- Internal control is the process established by an organization's board of directors, managers, and IT group to provide reasonable assurance for the effectiveness and efficiency of operations, the reliability of financial reporting, and compliance with applicable laws and regulations.
- Policies are the guidelines, standards, and laws by which the organization must abide. Policies drive processes and procedures. Processes are a collection of tasks designed to accomplish a stated objective. A procedure defines the exact instructions for completing each task in a process.
- A fundamental concept of good internal control is the careful separation of duties associated with any process that involves the handling of financial transactions so that different aspects of the process are handled by different people.
- In relationships between IT workers and other professionals, the priority is to improve the profession through activities such as mentoring inexperienced colleagues, demonstrating professional loyalty, and avoiding résumé inflation and the inappropriate sharing of corporate information.
- In relationships between IT professionals and IT users, important issues include software piracy, inappropriate use of IT resources, and inappropriate sharing of information.
- When it comes to the relationship between IT workers and society at large, the main challenge for IT workers is to practice the profession in ways that cause no harm to society and provide significant benefits.

Encouraging Professionalism of IT Workers

A professional is one who possesses the skill, good judgment, and work habits expected from a person who has the training and experience to do a job well.

Organizations—including many IT organizations—are desperately seeking workers who have the following characteristics of a professional:

- They are an expert in the tools and skills needed to do their job.
- They adhere to high ethical and moral standards.
- They produce high quality results.
- They meet their commitments.
- They communicate effectively.
- They train and develop others who are less skilled or experienced.

IT workers of all types can improve their profession's reputation for professionalism by:

1. Subscribing to a professional code of ethics
2. Joining and participating in professional organizations,
3. Obtaining appropriate certifications, and
4. Supporting government licensing where available.

Professional Codes of Ethics

A professional code of ethics states the principles and core values that are essential to the work of a particular occupational group. Practitioners in many professions subscribe to a code of ethics that governs their behavior.

For example, doctors adhere to varying versions of the 2,000-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 hopes 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. Nor can a professional code of ethics be expected to provide an answer to every ethical dilemma—no code can be a 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 acceptable and unacceptable behaviors 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 criticism.

Professional Organizations:

No one IT professional organization has emerged as preeminent, so there is no universal code of ethics for IT workers. However, the existence of such organizations is useful in a field that is rapidly growing and changing. In order to stay on the top of the many new developments in their field, IT workers need to network with others, seek out new ideas, and continually build on their personal skills and expertise. Whether you are a freelance programmer or the CIO of a Fortune 500 company, membership in an organization of IT workers enables you to associate with others of similar work experience, develop working relationships, and exchange ideas.

These organizations disseminate information through email, periodicals, websites, social media, meetings, and conferences. Furthermore, in recognition of the need for professional standards of competency and conduct, many of these organizations have developed codes of ethics.

Four of the most prominent IT-related professional organizations are highlighted below.

1. Association for Computing Machinery (ACM): It is computing society founded in New York in 1947, is “dedicated to advancing the art, science, engineering, and application of information technology, serving both professional and public interests by fostering the open interchange of information and by promoting the highest professional and ethical standards.” ACM is the world’s largest educational and scientific society and is international in scope, with ACM councils established in Europe, India, and China. Over half the organization’s 100,000 student and professional members reside outside the United States in more than 100 countries. Its leading magazine, *Communications of the ACM*, provides industry news, commentary, observations, and practical research. In addition, the ACM sponsors 37 special-interest groups (SIGs) representing major areas of computing. Each group provides publications, workshops, and conferences for information exchange.

2. Institute of Electrical and Electronics Engineers Computer Society (IEEE-CS): The Institute of Electrical and Electronics Engineers (IEEE) covers the broad fields of electrical, electronic, and information technologies and sciences. The IEEE-CS is one of the oldest and largest IT professional associations, with about 60,000 members. Founded in 1946, the IEEE-CS is the largest of the 38 societies of the IEEE. The

society sponsors many conferences, applications-related and research-oriented journals, local and student chapters, technical committees, and standards working groups.

3. Association of Information Technology Professionals (AITP): It started in Chicago in 1951, when a group of machine accountants got together and decided that the future was bright for the IBM punched-card tabulating machines they were operating—a precursor of the modern electronic computer. The AITP provides IT-related seminars and conferences, information on IT issues, and forums for networking with other IT workers. Its mission is to provide superior leadership and education in information technology, and one of its goals is to help members make themselves more marketable within their industry. The AITP also has a code of ethics and standards of conduct. The standards of conduct are considered to be rules that no true IT professional should violate.

4. SysAdmin, Audit, Network, and Security (SANS) Institute: SANS Institute provides information security training and certification for a wide range of individuals, such as auditors, network administrators, and security managers. Each year, its programs train some 12,000 people, and a total of more than 165,000 security professionals around the world have taken one or more of its courses. SANS publishes a semiweekly news digest (NewsBites), a weekly security vulnerability digest (@Risk), and flash security alerts. At no cost, SANS makes available a collection of some 1,200 research documents about various information security topics. SANS also operates Internet Storm Center—a program that monitors malicious Internet activity and provides a free early warning service to Internet users—and works with Internet service providers to thwart malicious attackers.

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 (for example, 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.

Deciding on the best IT certification—and even whether to seek a certification—depends on the individual's career aspirations, existing skill level, and accessibility to training.

Vendor Certifications: Many IT vendors—such as Cisco, IBM, Microsoft, SAP, and Oracle—offer certification programs for those who use their products. Workers who successfully complete a program can represent themselves 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.

Licensing of IT Professionals:

A government license is government-issued permission to engage in an activity or to operate a business. Most states license activities that could result in damage to public health, safety, or welfare—if practiced by an individual who has not demonstrated minimal competence.

Licensing 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 daycare providers, and some engineers.

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, and every day, the public entrust their health, safety, and welfare to these systems.
- Software systems are embedded in the vehicles we drive, controlling functions such as braking, cruise control, airbag deployment, navigation, and parking. Even more advanced systems are being designed and built for “self-driving” vehicles.
- Complex computers and information systems manage and control the autopilot functions of passenger planes, the nuclear reactors of power plants, and the military’s missile launch and guidance systems.
- Complex medical information systems monitor hospital patients on critical life support.
- Failure of any of these systems can result in human injury or even death.
- 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. Without licensing, there are no clear, well-defined requirements for heightened care and no concept of professional malpractice.
- State licensing boards have ultimate authority over the specific requirements for licensing in their jurisdiction, and also decide whether or not to even offer a given exam.

In 2013, NCEES (National Council of Examiners for Engineering and Surveying (NCEES) develops, administers, and scores the examinations used for engineering and surveying licensure in the United States.) began offering testing for software engineers. The eight-hour exam consisting of 80 multiple-choice questions was produced in collaboration with the Institute of Electrical and Electronic Engineers (IEEE). As of 2015, 40 states and U.S. jurisdictions support the licensing of software engineers. The software engineering license certifies that the license holder has:

1. completed an appropriate engineering education from a program accredited by the Accreditation Board for Engineering and Technology/Engineering Accreditation. (As of October 2015, there are 23 accredited software engineering programs in the United States and 239 computer engineering programs in the United States.)
2. at least four years of software engineering experience in his or her field (the required years of experience varies by state) working under the supervision of qualified engineers.
3. passed the following two NCEES engineering exams:
 - i) the Fundamentals of Engineering exam, which is a broad-based exam and
 - ii) an eight-hour software engineering Principles and Practices exam, which covers topics such as software requirements, design, construction, testing, maintenance, configuration management, engineering processes, quality assurance, safety, security, and privacy.
4. kept current by meeting his or her state’s minimum continuing education requirements

IT Professional Malpractice

For most IT workers, becoming licensed as a software engineer is optional because they practice under the “industrial exemption” clause of their state’s licensing laws that permits them to work internally for an organization without licensure so long as they are not making final decisions to release product to the public or offering engineering services directly to the public (for example, software engineering consultant). However, to open a software engineering consulting practice or to claim that one is a software engineer in a formal context may now require a license in some states. For an IT worker to become licensed raises some potential legal issues, as discussed in the following paragraphs.

Negligence is defined as not doing something that a reasonable person would do or doing something that a reasonable person would not do. Duty of care refers 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.

The courts decide whether parties owe a duty of care by applying a reasonable person standard to evaluate how an objective, careful, and conscientious person would have acted in the same circumstances. Likewise, defendants who have particular expertise or competence are measured against a reasonable professional standard.

For example: A hypothetical negligence case in which an employee inadvertently destroyed millions of customer records in an Oracle database. The standard of measure would be higher if the defendant were a licensed software engineer certified as an Oracle database administrator (DBA) with 10 years of experience rather than an unlicensed systems analyst with no DBA experience or specific knowledge of the Oracle software. If a court finds that a defendant actually owed a duty of care, it must then determine whether the duty was breached.

A breach of the duty of care is the failure to act as a reasonable person would act. A breach of duty might consist of an action, such as throwing a lit cigarette into a fireworks factory and causing an explosion, or a failure to act when there is a duty to do so—for example, a police officer not protecting a citizen from an attacker.

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

Summary

What can be done to encourage the professionalism of IT workers?

- A professional is one who possess the skill, good judgment, and work habits expected from a person who has the training and experience to do a job well.
- A professional is expected to contribute to society, to participate in a lifelong training program, to keep abreast of developments in the field, and to help develop other professionals.
- IT workers of all types can improve their profession’s reputation for professionalism by:
 - i) subscribing to a professional code of ethics,
 - ii) joining and participating in professional organizations,
 - iii) obtaining appropriate certifications, and
 - iv) supporting government licensing where available.
- A professional code of ethics states the principles and core values that are essential to the work of a particular occupational group.
- Codes of ethics usually have two main parts—the first outlines what the organization aspires to become and the second typically lists rules and principles that members are expected to live by.

The codes also typically include a commitment to continuing education for those who practice the profession.

- Adherence to a code of ethics can produce many benefits for the individual, the profession, and society as a whole, including ethical decision making, high standards of practice and ethical behavior, trust and respect with the general public, and access to an evaluation benchmark that can be used for self-assessment.
- Several IT-related professional organizations have developed a code of ethics, including ACM, IEEE-CS, AITP, and SANS.
- Many people believe that the licensing and certification of IT workers would increase the reliability and effectiveness of information systems.
- Certification indicates that a professional possesses a particular set of skills, knowledge, or abilities, in the opinion of the certifying organization. Numerous companies and professional organization offer certification.
- Most states support the licensing of software engineers, and the state licensing boards have ultimate responsibility over specific requirements for licensing in their jurisdiction.

Encouraging ethical use of IT resources among users

The ethical use of IT resources among users is the area of growing concern as more companies provide employees with smartphone, tablets, and laptops along with desktop PC and other devices – to access corporate information system.

Some of the common ethical issues with IT users are:

1. Software piracy
2. Inappropriate use of computing resources
3. Inappropriate sharing of Information

Software piracy: 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.

The increasing popularity of the Android smartphone operating system has created a serious software piracy problem. Some IT end users have figured out how to download applications from the Google Play store without paying for them, and then use the software or sell it to others. Software piracy can have a negative impact on future software development if professional developers become discouraged watching revenue from legitimate sales sink while the sales of pirated software and games skyrocket.

Inappropriate Use of Computing Resources: Some employees use their computers to surf popular websites that have nothing to do with their jobs, participate in chat rooms, view pornographic sites, and play computer games.

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

Inappropriate Sharing of Information: Every organization stores vast amounts of information that can be classified as either private or confidential.

Private data describe individual employees—for example, their salary information, attendance data, health records, and performance ratings. Private data also include 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 employee accessed a coworker's payroll records via a human resources computer system and then discussed them with a friend, it would be a clear violation of the coworker's privacy.

One of the most serious leaks of sensitive information in the U.S. history occurred in late 2010, when hundreds of thousands of leaked State Department documents were posted on the WikiLeaks' website. The source of the leaks was a low-level IT user (an army private) with access to confidential documents. The documents revealed details of behind-the-scenes international diplomacy, often divulging candid comments from world leaders and providing particulars of U.S. tactics in Afghanistan, Iran, and North Korea. The leaked documents strained relations between the United States and some of its allies. It is also possible that the incident will cause other countries to be less willing to share sensitive information with the United States because of concerns over further disclosures.

Supporting the Ethical Practices of IT Users

The growing use of IT has increased the potential for new ethical issues and problems; thus, many organizations have recognized the need to develop policies that protect against abuses. Although no policy can stop wrongdoers, it can set forth the general rights and responsibilities of all IT users, establish boundaries of acceptable and unacceptable behavior, and enable management to punish violators.

Loyalty to a policy can improve services to users, increase productivity, and reduce costs. Companies can take several actions when creating an IT usage policy, as discussed below:

1. Establishing Guidelines for Use of Company Hardware and Software: Company IT managers must provide clear rules that govern the use of home computers and associated software. Some companies negotiate contracts with software manufacturers and provide PCs and software so that IT users can work at home. Other companies help employees buy hardware and software at corporate discount rates. The goal should be to ensure that employees have legal copies of all the software they need to be effective, regardless of whether they work in an office, on the road, or at home.

2. Defining an Acceptable Use Policy: An acceptable use policy (AUP) is a document that specifies restrictions and practices that a user must agree to in order to use organizational computing and network resources. It is an essential information security policy—so important that most organizations require that employees sign an acceptable use policy before being granted a user or network ID. An effective acceptable use policy is clear and concise and contains the following five key elements:

- i) Purpose of the AUP—Why is the policy needed and what are its goals?
- ii) Scope—Who and what is covered under the AUP?
- iii) Policy—How are both acceptable use and unacceptable use defined; what are some examples of each?
- iv) Compliance—Who is responsible for monitoring compliance and how will compliance will be measured?
- v) Sanctions—What actions will be taken against an individual who violates the policy?

Members of the legal, human resources, and information security groups are involved in creating the AUP. It is the organization's information security group that is responsible for monitoring compliance to the

AUP. Information security (infosec) group's responsibilities include managing the processes, tools, and policies necessary to prevent, detect, document, and counter threats to digital and nondigital information, whether it is in transit, being processed, or at rest in storage.

3. Structuring Information Systems to Protect Data and Information: Organizations must implement systems and procedures that limit data access to just those employees who need it.

For example, sales managers may have total access to sales and promotion databases through a company network, but their access should be limited to products for which they are responsible. Furthermore, they should be prohibited from accessing data about research and development results, product formulas, and staffing projections if they don't need it to do their jobs.

4. Installing and Maintaining a Corporate Firewall: A firewall is hardware or software (or a combination of both) that serves as the first line of defense between an organization's network and the Internet; a firewall also limits access to the company's network based on the organization's Internet-usage policy. A firewall can be configured to serve as an effective deterrent to unauthorized web surfing by blocking access to specific objectionable websites. (Unfortunately, the number of such sites is continually growing, so it is difficult to block them all.) A firewall can also serve as an effective barrier to incoming email from certain websites, companies, or users. It can even be programmed to block email with certain kinds of attachments (for example, Microsoft Word documents), which reduces the risk of harmful computer viruses.

5. Compliance: Compliance means to be in accordance with established policies, guidelines, specifications, or legislation. Commercial software used within an organization should be distributed in compliance with the vendor's licensing agreement. In the legal system, compliance usually refers to behavior in accordance with legislation. Failure to be in compliance with specific pieces of legislation can lead to criminal or civil penalties specified in that legislation. Failure to be in compliance with legislation can also lead to lawsuits or government fines.

Summary

What ethical issues do IT users face, and what can be done to encourage their ethical behavior?

- IT users face several common ethical issues, including software piracy, inappropriate use of computing resources, and inappropriate sharing of information.
- Actions that can be taken to encourage the ethical behavior of IT users include establishing guidelines for the use of company hardware and software; defining an AUP for the use of IT resources; structuring information systems to protect data and information; installing and maintaining a corporate firewall; and ensuring compliance with laws, policies, and standards.
- The information security (infosec) group is responsible for managing the processes, tools, and policies necessary to prevent, detect, document, and counter threats to digital and nondigital information.
- The audit committee of a board of directors and members of the internal audit team have a major role in ensuring that both the IT organization and IT users are in compliance with organizational guidelines and policies as well as various legal and regulatory practices.

Practice Questions:

1. What does it mean for an organization to act ethically? How can one evaluate whether this is the case?
2. It is easy to say that an organization should hire, reward, and dismiss employees based on their character as well as their knowledge and skill, but how could such a policy be implemented?
3. It is common practice for managers to hold people accountable to meet “stretch” goals, quotes, and budgets. Can this be done in a way that does not encourage unethical behavior on the part of employees? Defend your response.
4. What characteristics would you say are true earmarks of an employee who is unprofessional in his or her approach to work?
5. Do you believe that software manufacturers should be tolerant of the practice of software piracy in third-world countries to allow these countries an opportunity to move more quickly into the information age? Why or why not?
6. Describe a situation in which there could be a conflict of interest between an IT consultant’s self-interest and the interests of a client. How might this potential conflict be addressed?
7. Should software developers who work on critical applications whose failure could result in loss of human life (for example, software for self-driving cars) be required to be licensed? Why or why not?
8. What do you think are the benefits you can derive from joining a professional organization for people in your chosen career field?
9. What certifications are available for someone in your chosen career field? Which of these are considered most valuable?
10. What is the difference between a breach of duty of care and professional malpractice?