LESSON NINE: LEGAL AND ETHICAL CONSIDERATIONS

As with any other business activity, e-business must adhere to legal and ethical codes. However, e-business entails some new legal and ethical issues of which managers must be aware, including the following:

- Privacy
- Intellectual Property Right
- Legal Jurisdiction
- Content Regulation

PRIVACY

Privacy includes freedom from intrusion, the right to be left alone, the right to control information about oneself, and freedom from surveillance. It is a major issue in e-business because of the widespread availability of personal data and the ease of tracking a person's activities on the Internet. Several countries have enacted laws to control certain types of personal information, such as medical, credit, and other financial information. These laws carry over to the e-business environment. As companies build large database on their e-business customers, the values of this data makes the selling of the data an attractive business option. Internet technologies, cookies in particular, make tracking the browser activities of individuals possible. Consumer concerns about this perceived invasion of privacy is requiring companies to post and adhere to privacy statements on their Websites.

INTELLECTUAL PROPERTY RIGHT

The protection of Intellectual property is critical to e-business because many products and services contain Intellectual property, copies are easy to make, and the copy is as good as the original. Example of e-business activities in which Intellectual property right are critical include electronic publishing, software distribution, virtual art galleries, music distribution over the Internet, and inline education.

are four types of legal protection of Intellectual property:

copyrights, patents, trademarks, and trade secrets.

a. Copyright.

Copyright law aims to protect an author's or Artist's expression once it is in tangible form. The work must be expressive rather than functional; a copyright protect the expression, not the idea. For example, a cartoon duck is an idea and cannot be copyrighted, but Donald Duck and Daffy Duck are expressions of that idea and are copyrighted. Registering a copyright is not a requirement; putting the expression into tangible form is sufficient.

Just about all original content on a website can be copyrighted by the creator of the site, from buttons to video, from text to site layouts. If a company hires someone to develop a site, by default, the copyright belongs to the developer, not the company. The developer can then demand royalties from the company if it uses the Website; therefore it behaves companies to clearly define the ownership of the copyright in the contract.

b. Patents.

Patent law aims to protect inventions - things or processes for producing things - that is, "anything under the sun made by man" but not "abstract idea" or natural laws, according to U.S. copyright law. Valid for 20years, the protection is quite strong. In the United States, patents are granted by the U.S. Patent and Trademark Office after stringent thresholds on inventiveness have been met. The United States recognizes patents for business processes. Although software, in general, cannot be patented - it must be copyrighted - certain business practices implemented in software can be patented. In the e-business area, Amazon.com has received a patent for "one click purchasing." The company has enforced its patent rights against its main competitor, Barnes and Noble cannot use one click purchasing on its Website. British Telecom has claimed to have invented the hyperlink. To obtain the patent, the company will have show that no prior use of hyperlinks occurred before its use. Any prior use would invalidate the patent.

c. Trademark.

Trademarks protect names, symbols, and other icons used to identify a company or product. Trademarks can be registered with the U.S. Patent and Trademark Office. A trademark is a valid indefinitely, as long as it is used and does not become a generic name for the goods or services. The aim of trademark law is to prevent confusion among consumers in a market with similar identifying names or symbols. The standard for trademark infringement is whether the marks are "confusingly similar."

The biggest area of trademark conflicts in e-business has to do with domain name registration.

d. Trade secret.

Trade secret, as the name implies, protect company secrets, which can cover a wide range of processes, formulas, and techniques. A trade secret is not registered and is valid indefinitely, as long as it remains a secret. Although laws protect against the theft of trade secrets, it is not illegal to discover a trade secret through reverse engineering. Trade secrets are the area of Intellectual property rights least application to e-business.

ETHICS

Principles of right and wrong that individuals, acting as free moral agents, use to make choices to guide their behavior.

Information systems and ethics

Information systems raise new ethical questions because they create opportunities for:

- Intense social change, threatening existing distributions of power, money, rights and obligations
- New kinds of crime

Ethical, Social, and Political IT Issues

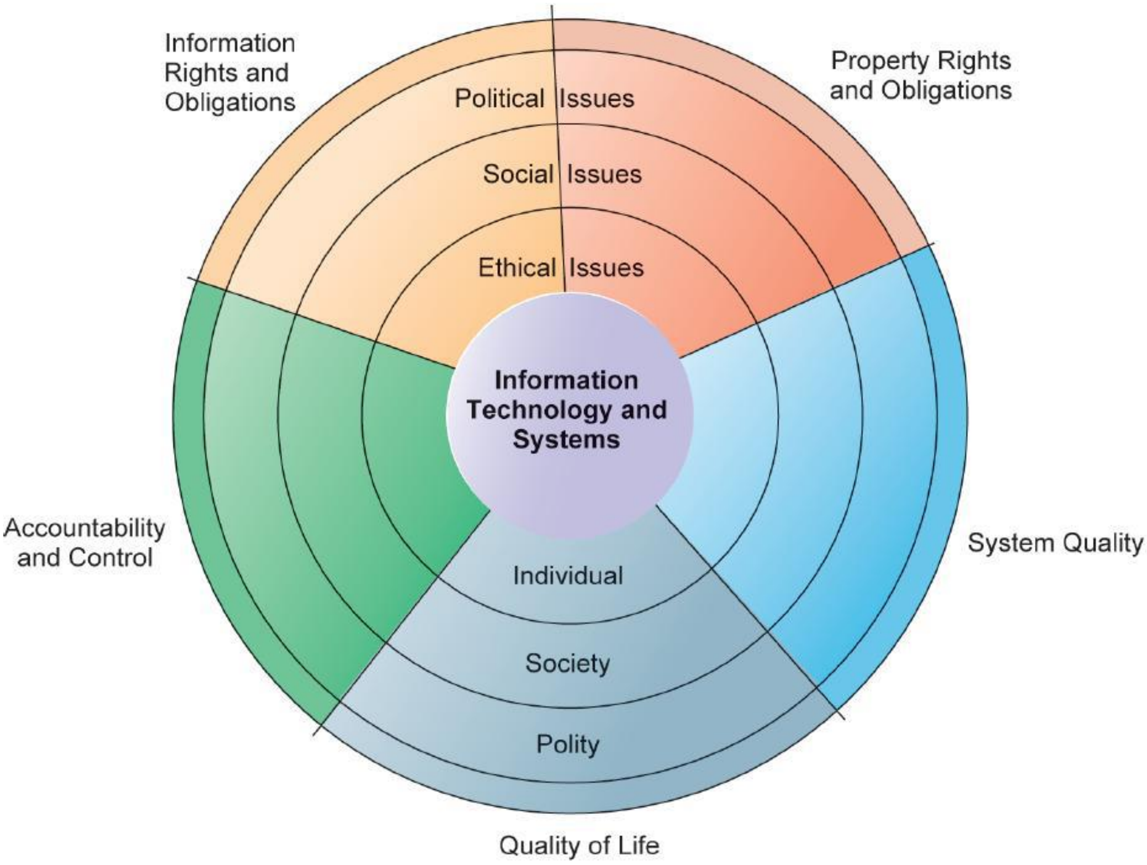
Major issues raised by information systems ripples include:

- Information rights and obligations
- Property rights and obligations
- Accountability and control
- System quality
- Quality of life

A model for thinking about ethical, social, and political issues

Ethical, social, and political issues are closely linked. The ethical dilemma you may face as a manager of information systems typically is reflected in social and political debate. One way to think about these relationships is given in Figure shown below. Imagine society as a more or less calm pond on a summer day, a delicate ecosystem in partial equilibrium with individuals and with social and political institutions. Individuals know how to act in this pond because social institutions (family, education, organizations) have developed well-honed rules of behavior, and these are supported by laws developed in the political sector that prescribe behavior and promise sanctions for violations. Now toss a rock into the center of the pond. But imagine instead of a rock that the disturbing force is a powerful shock of new information technology and systems hitting a society more or less at rest. What happens? Ripples, of course.

Figure showing the relationship between ethical, social, and political issues in an information society


Information Rights and Obligations
Property Rights and Obligations
Political Issues
Social Issues
Ethical Issues
Information Technology and Systems
Accountability and Control
System Quality
Individual
Society
Polity
Quality of Life

Five moral dimensions of the information age

The major ethical, social, and political issues raised by information systems include the following moral dimensions:

1.Information rights and obligations. What **information rights** do individuals and organizations possess with respect to themselves? What can they protect? What obligations do individuals and organizations have concerning this information?

2. Property rights and obligations. How will traditional intellectual property rights be protected in a digital society in which tracing and accounting for ownership are difficult and ignoring such property rights is so easy?

3. Accountability and control. Who can and will be held accountable and liable for the harm done to individual and collective information and property rights?

4. System quality. What standards of data and system quality should we demand to protect individual rights and the safety of society?

5. Quality of life. What values should be preserved in an information- and knowledge-based society? Which institutions should we protect from violation?

Which cultural values and practices are supported by the new information technology?

ETHICS IN AN INFORMATION SOCIETY

Ethics is a concern of humans who have freedom of choice. Ethics is about individual choice: When faced with alternative courses of action, what is the correct moral choice? What are the main features of ethical choice?

BASIC CONCEPTS: RESPONSIBILITY, ACCOUNTABILITY, AND LIABILITY

Ethical choices are decisions made by individuals who are responsible for the consequences of their actions.

- **Responsibility** is a key element of ethical action. Responsibility means that you accept the potential costs, duties, and obligations for the decisions you make.

- **Accountability** is a feature of systems and social institutions: It means that mechanisms are in place to determine who took responsible action, who is responsible. Systems and institutions in which it is impossible to find out who took what action are inherently incapable of ethical analysis or ethical action.

- **Liability** is a feature of political systems in which a body of laws is in place that permits individuals to recover the damages done to them by other actors, systems, or organizations.

ETHICAL ANALYSIS

When confronted with a situation that seems to present ethical issues, how should you analyze it? The following five-step process should help.

1. Identify and describe clearly the facts. Find out who did what to whom, and where, when, and how. In many instances, you will be surprised at the errors in the initially reported facts, and often you will find that simply getting the facts straight helps define the solution. It also helps to get the opposing parties involved in an ethical dilemma to agree on the facts.

2. Define the conflict or dilemma and identify the higher-order values involved. Ethical, social, and political issues always reference higher values. The parties to a dispute all claim to be pursuing higher values (e.g., freedom, privacy, protection of property, and the free enterprise system). Typically, an ethical issue involves a dilemma: two diametrically opposed courses of action that support worthwhile values. For example, the chapter-ending case study illustrates two competing values: the need to protect citizens from terrorist acts and the need to protect individual privacy.

3. Identify the stakeholders. Every ethical, social, and political issue has stakeholders: players in the game who have an interest in the outcome, who have invested in the situation, and usually who have vocal opinions. Find out the identity of these groups and what they want. This will be useful later when designing a solution.

4. Identify the options that you can reasonably take. You may find that none of the options satisfy all the interests involved, but that some options do a better job than others. Sometimes arriving at a good or ethical solution may not always be a balancing of consequences to stakeholders.

***5. Identify the potential consequences of your options*.** Some options may be ethically correct but disastrous from other points of view. Other options may work in one instance but not in other similar instances. Always ask yourself, “What if I choose this option consistently over time?”

LESSON 10: INFORMATION SYSTEM SECURITY

The term security is easiest to define by breaking it into pieces. An **information system** consists of the hardware, operating system, and application software that work together to collect, process, and store data for individuals and organizations.

Security as a condition is the degree of resistance to, or protection from, harm. It applies to any vulnerable and valuable asset, such as a person, dwelling, community, nation, or organization. Establishing or maintaining a sufficient degree of security is the aim of the work, structures, and processes called "security."

Thus **information systems security** is the collection of activities that protect the information system and the data stored in it. **Information security** means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Adversaries of information system security

To understand how to make computers more secure, you first need to understand the concepts of risks, threats, and vulnerabilities.

- **Risk** is the likelihood that something bad will happen to an asset. It is the level of exposure to some event that has an effect on an asset. In the context of IT security, an asset can be a computer, a database, or a piece of information. Examples of risk include the following:
    - Losing data
    - Losing business because a disaster has destroyed your building
    - Failing to comply with laws and regulations

It has two components:

Risk Exposure = Probability * Damage Potential (Consequence/loss)

This formula indicates that the risk posed by a particular threat is equal to the probability of the threat occurring multiplied by the damage potential, which indicates the consequences to your system if an attack were to occur.

- **A threat** is any action that could damage an asset. Information systems face both natural and human-induced threats. The threats of flood, earthquake, or severe storms require organizations to create plans to ensure that business operation continues and that the organization can recover. A business continuity plan (BCP) gives priorities to the functions an organization needs to keep going. A disaster recovery plan (DRP) defines how a business gets back on its feet after a major disaster such as a fire or hurricane. Human-caused threats to a computer system include viruses, malicious code, and unauthorized access. A virus is a computer program written to cause damage to a system, an application, or data. Malicious code, or malware, is a computer program written to cause a specific action to occur, such as erasing a hard drive. These threats can harm an individual, business, or organization.

- **A vulnerability** is a weakness that allows a threat to be realized or to have an effect on an asset. To understand what a vulnerability is, think about lighting a fire. Lighting a fire is not necessarily bad. If you are cooking a meal on a grill, you will need to light a fire in the grill. The grill is designed to contain the fire and should pose no danger if used properly. On the other hand, lighting a fire in a computer data center will likely cause damage. A grill is not vulnerable to fire, but a computer data center is. A threat by itself does not always cause damage; there must be a vulnerability for a threat to be realized.

CORE PRINCIPLES OF INFORMATION SECURITY

i. Confidentiality

Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems. For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred.

Breaches of confidentiality take many forms. Permitting someone to look over your shoulder at your computer screen while you have confidential data displayed on it could be a breach of confidentiality. If a laptop computer containing sensitive information about a company's employees is stolen or sold, it could result in a breach of confidentiality. Giving out confidential information over the telephone is a breach of confidentiality if the caller is not authorized to have the information.

Confidentiality is necessary (but not sufficient) for maintaining the privacy of the people whose personal information a system holds.

ii. Integrity

In information security, integrity means that data cannot be modified undetectably. This is not the same thing as referential integrity in databases, although it can be viewed as a special case of Consistency as understood in the classic ACID model of transaction processing. Integrity is violated when a message is actively modified in transit. Information security systems typically provide message integrity in addition to data confidentiality.

iii. Availability

For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks.

iv. Authenticity

In computing, e-Business and information security it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim they are.

v. Non-repudiation

In law, non-repudiation implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction.

Electronic commerce uses technology such as digital signatures and encryption to establish authenticity and non-repudiation.

CONTROLS

When Management chooses to mitigate a risk, they will do so by implementing one or more of three different types of controls.

i. Administrative Controls

Administrative controls (also called procedural controls) consist of approved written policies, procedures, standards and guidelines. Administrative controls form the framework for running the business and managing people. They inform people on how the business is to be run and how day to day operations are to be conducted. Laws and regulations created by government bodies are also a type of administrative control because they inform the business. Some industry sectors have policies, procedures, standards and guidelines that must be followed - the Payment Card Industry (PCI) Data Security Standard required by Visa and Master Card is such an example. Other examples of administrative controls include the corporate security policy, password policy, hiring policies, and disciplinary policies.

Administrative controls form the basis for the selection and implementation of logical and physical controls. Logical and physical controls are manifestations of administrative controls. Administrative controls are of paramount importance.

ii. Logical controls

Logical controls (also called technical controls) use software and data to monitor and control access to information and computing systems. For example: passwords, network and host based firewalls, network intrusion detection systems, access control lists, and data encryption are logical controls.

An important logical control that is frequently overlooked is the principle of least privilege. The principle of least privilege requires that an individual, program or system process is not granted any more access privileges than are necessary to perform the task. A blatant example of the failure to adhere to the principle of least privilege is logging into Windows as user Administrator to read Email and surf the Web. Violations of this principle can also occur when an individual collects additional access privileges over time. This happens when employees' job duties change, or they are promoted to a new position, or they transfer to another department. The access privileges required by their new duties are frequently added onto their already existing access privileges which may no longer be necessary or appropriate.

iii. Physical Control

Physical controls monitor and control the environment of the work place and computing facilities. They also monitor and control access to and from such facilities. For example: doors, locks, heating and air conditioning, smoke and fire alarms, fire suppression systems, cameras, barricades, fencing, security guards, cable locks, etc. Separating the network and work place into functional areas are also physical controls.

An important physical control that is frequently overlooked is the separation of duties. Separation of duties ensures that an individual cannot complete a critical task by himself. For example: an employee who submits a request for reimbursement should not also be able to authorize payment or print the check. An applications programmer should not also be the server administrator or the database administrator - these roles and responsibilities must be separated from one another.

Scenario for Understanding Legal, Ethical, and Security Considerations in E-Business

Scenario: E-Commerce Platform Facing Legal, Ethical, and Security Challenges

Background:

LUMINOUS Electronics, a growing e-commerce business, sells electronics and gadgets online. The company has been expanding rapidly, acquiring more customers and handling large amounts of sensitive customer data, including personal details, financial transactions, and browsing history.

While LUMINOUS Electronics is benefiting from digital transformation, it faces several legal, ethical, and security challenges that could affect its business operations.

A. Legal and Ethical Considerations

1. Privacy Issue – Selling Customer Data

LUMINOUS Electronics collects customer browsing behavior, purchase history, and contact information through its website. The marketing team sells this data to third-party advertisers without obtaining proper consent from users.

Questions:

- What ethical and legal issues does LUMINOUS Electronics face regarding customer privacy?
- What laws and ethical principles should the company follow to protect user privacy?
- How can the company ensure compliance with privacy regulations like GDPR or Kenya's Data Protection Act?

2. Intellectual Property Rights – Copyright and Trademark Infringement

The company hired a web developer to create its website and product descriptions. However, the developer did not transfer copyright ownership of the website content to LUMINOUS Electronics. Later, the developer demanded royalty payments for the continued use of the website.

Additionally, LUMINOUS Electronics used images and product descriptions from a competitor’s website without permission, leading to a copyright dispute.

Questions:

- Who owns the intellectual property of the website, and what legal risks does LUMINOUS Electronics face?
- What should LUMINOUS Electronics have done before signing a contract with the developer?

- How can LUMINOUS Electronics legally protect its brand, trademarks, and copyrighted content?

3. Legal Jurisdiction – International Sales Disputes

A customer from Germany purchases a smartphone from LUMINOUS Electronics, but upon delivery, the product is faulty. The customer files a lawsuit in Germany, but LUMINOUS Electronics is based in Kenya and operates under Kenyan business laws.

Questions:

- What legal jurisdiction applies in cross-border e-commerce transactions?
- How should LUMINOUS Electronics handle legal disputes involving international customers?
- What steps can LUMINOUS Electronics take to protect itself from international legal conflicts?

B. Ethical Issues in Information Systems

4. System Integrity – Fake Product Reviews & False Advertising

To attract more buyers, LUMINOUS Electronics pays employees to write fake positive reviews for products. Additionally, some products are advertised as having longer battery life than they actually do.

Questions:

- What ethical concerns arise from fake reviews and false advertising?
- How do misleading business practices impact customer trust and brand reputation?
- What ethical principles should guide LUMINOUS Electronics' marketing strategies?

5. Cybersecurity Risk – Customer Data Breach

A hacker gains access to LUMINOUS Electronics’ database and steals customer payment information and passwords. The company does not immediately inform customers to avoid bad publicity. Later, customers report fraudulent transactions, and LUMINOUS Electronics faces lawsuits for failing to disclose the breach.

Questions:

- What are the legal and ethical responsibilities of LUMINOUS Electronics in case of a data breach?
- How should the company handle cyber incidents to ensure compliance with data protection laws?
- What security measures can LUMINOUS Electronics implement to prevent future cyber-attacks?

C: Information System Security Issues

6. Threats to Information Security – Cyber Attacks & Fraudulent Transactions

LUMINOUS Electronics experiences:

Phishing Attacks: Customers receive fake emails requesting login details.

Ransomware Attack: Hackers encrypt company files and demand a ransom.

Fake Transactions: Fraudsters use stolen credit cards to place orders.

Questions:

- Identify three key security threats LUMINOUS Electronics faces and explain how they affect business operations.
- How can LUMINOUS Electronics improve its security policies to prevent cyber attacks?
- What risk management strategies should be implemented to protect customer data and financial transactions?

7. Implementing Information Security Controls

To enhance security, LUMINOUS Electronics must implement the following:

Administrative Controls: Employee training on cybersecurity and legal compliance.

Logical Controls: Firewalls, encryption, and multi-factor authentication (MFA).

Physical Controls: Secure server rooms, biometric access, and surveillance cameras.

Questions:

- How can each type of security control (Administrative, Logical, Physical) protect LUMINOUS Electronics?
- What security best practices should LUMINOUS Electronics enforce to ensure data confidentiality, integrity, and availability?
- How does ensuring information security contribute to customer trust and business success?

Final Reflection Questions:

- What lessons can businesses learn from **LUMINOUS Electronics' legal, ethical, and security challenges**?
- What real-world **case studies** demonstrate similar **issues and solutions**?
- If you were a manager at LUMINOUS Electronics, how would you **implement a compliance and security framework**?