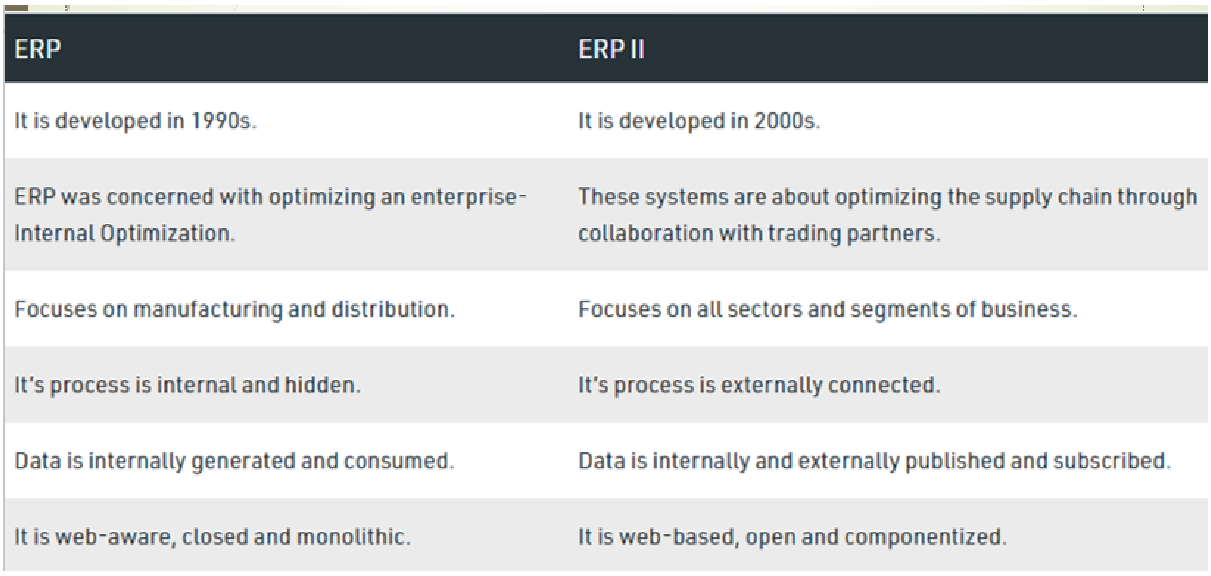
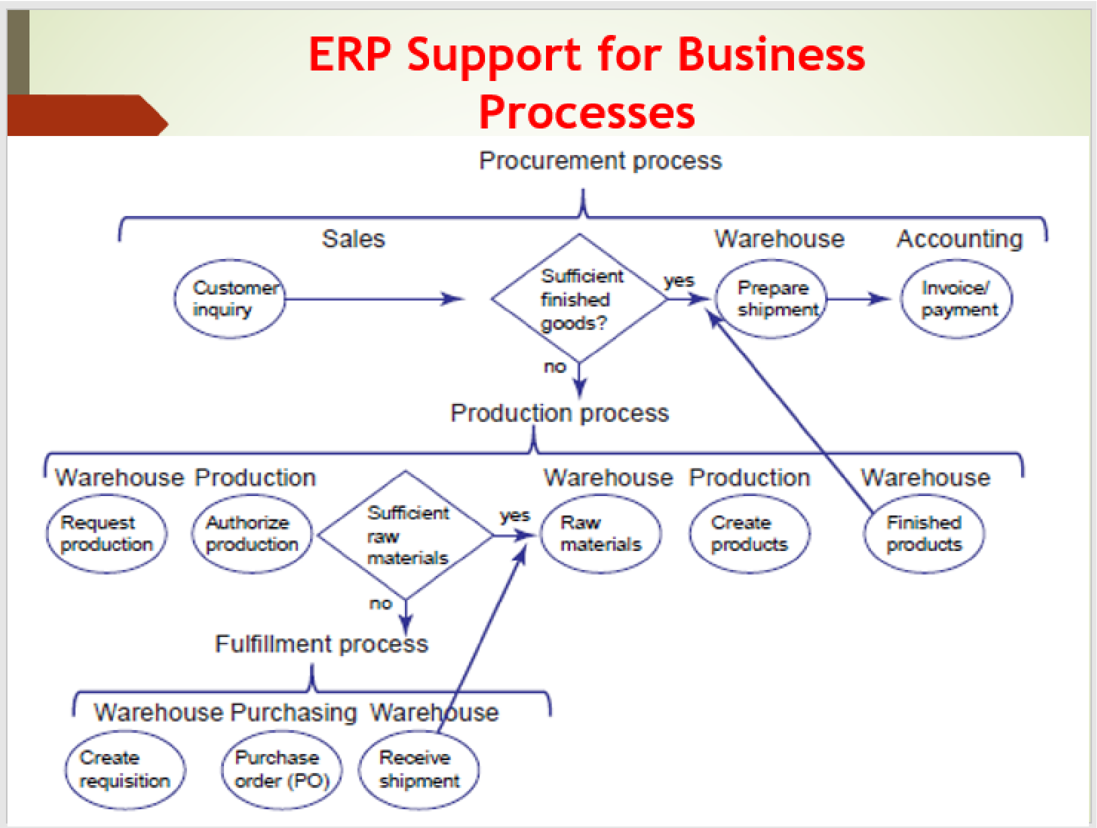
Module 3

Q1 Difference between ERP I & ERP II.



ERP	ERP II
It is developed in 1990s.	It is developed in 2000s.
ERP was concerned with optimizing an enterprise-Internal Optimization.	These systems are about optimizing the supply chain through collaboration with trading partners.
Focuses on manufacturing and distribution.	Focuses on all sectors and segments of business.
It's process is internal and hidden.	It's process is externally connected.
Data is internally generated and consumed.	Data is internally and externally published and subscribed.
It is web-aware, closed and monolithic.	It is web-based, open and componentized.

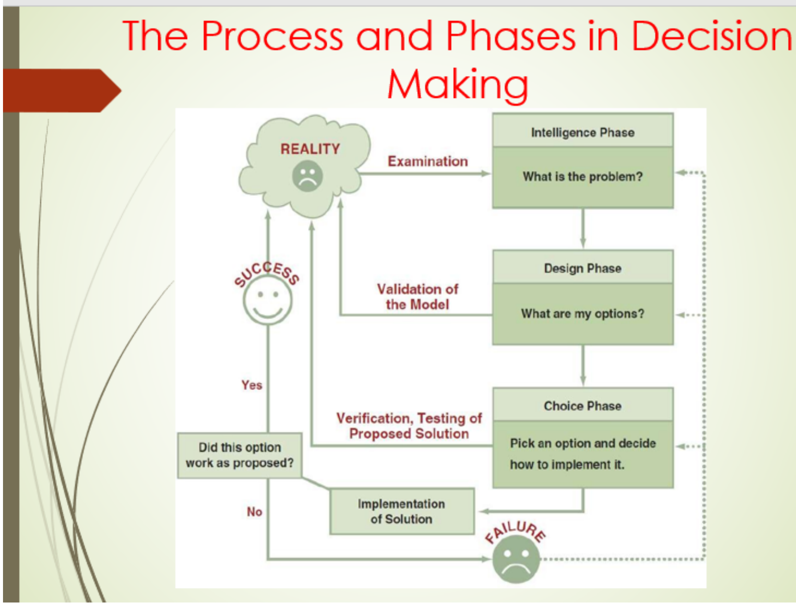
Q2 Explain ERP support for business processes?



ERP Support for Business Processes

Q3 Why are ERP upgrades so complex and expensive?

Q4 Identify the phases in the decision-making process, and use a decision support framework to demonstrate how technology supports managerial decision making.



The Process and Phases in Decision Making

REALITY

Examination

Intelligence Phase

What is the problem?

Design Phase

What are my options?

Validation of the Model

SUCCESS

Yes

Choice Phase

Pick an option and decide how to implement it.

Verification, Testing of Proposed Solution

Did this option work as proposed?

Implementation of Solution

No

FAILURE

Q5 How will you use the BI technique to improvise the business by knowing the customer's behaviour? Explain with a detailed example.

Q6Describe and provide examples of the three different ways in which organisations use business intelligence (BI)

Q7 What are the different commercial application of AI

Q8 What is an expert system? What are the different components of an expert system?

Q9 What are the major applications where expert systems can be implemented?

- **MYCIN –**

  One of the earliest expert systems based on backward chaining. It can identify various bacteria that can cause severe infections and can also recommend drugs based on the person's weight.
- **DENDRAL –**

  It was an artificial intelligence-based expert system used for chemical analysis. It used a substance's spectrographic data to predict its molecular structure.
- **R1/XCON –**

  It could select specific software to generate a computer system wished by the user.

- **PXDES –**

  It could easily determine the type and the degree of lung cancer in a patient based on the data.
- **CaDet –**

  It is a clinical support system that could identify cancer in its early stages in patients.
- **DXplain –**

  It was also a clinical support system that could suggest a variety of diseases based on the findings of the doctor.

Q10 Explain the different tools (Neural Network, Fuzzy logic, Genetic Algorithm, VR) used to develop cognitive science applications.

11 What are the differences between new AI based applications versus old decision making systems?

Q12 What are some of the limitations or dangers you see in the use of AI technologies such as expert systems, virtual reality, and intelligent agents?

Q13 One difference between a conventional business intelligence system and an expert system is that the former can explain how questions, whereas the latter can explain both how and why questions. Discuss the implications of this statement.

Q14 Explain the potential value and the potential limitations of artificial intelligence.

Q15 Provide examples of the benefits, applications, and limitations of expert systems.

Q16 Explain how your university could employ an expert system in its admission process. Could it use a neural network? What might happen if a student were denied admission to the university and his parents discovered that an expert system was involved in the admissions process?

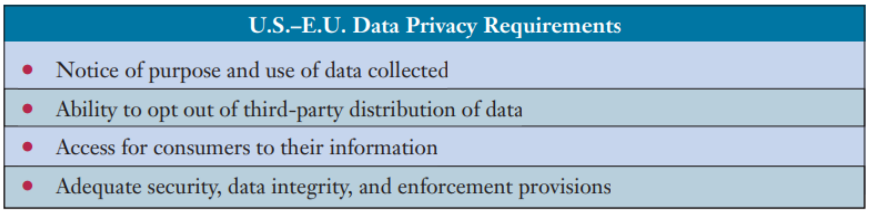
Module 4

1. Discuss how privacy issues can impact transborder data flows.

Transborder data flows (TDF), in which business data flow across international borders over the telecommunications networks of global information systems. Many countries view TDF as a violation of their national sovereignty because these data flows avoid customs duties and regulations for the import or export of goods and services. Others view TDF as a violation of their laws to protect the local IT industry from competition or their labor regulations for protecting local jobs. In many cases, the data flow business issues that seem especially politically sensitive are those that affect the movement out of a country of personal data in e-commerce and human resource applications. Many countries, especially those in the European Union (E.U.), may view transborder data flows as a violation of their privacy legislation because, in many cases, data about individuals are being moved out of the country without stringent privacy safeguards. For example, Figure 14.19outlines the key provisions of a data privacy agreement between the United States and the European Union. The agreement exempts U.S. companies engaging in international e-commerce from E.U. data privacy sanctions if they join a self-regulatory program that provides E.U. consumers with basic information about, and control over, how their personal data are used. Thus, the agreement is said to provide a “safe harbor” for such companies from the requirements of the E.U.’s Data Privacy Directive, which bans the transfer of personal information on E.U. citizens to countries that do not have adequate data privacy protection.

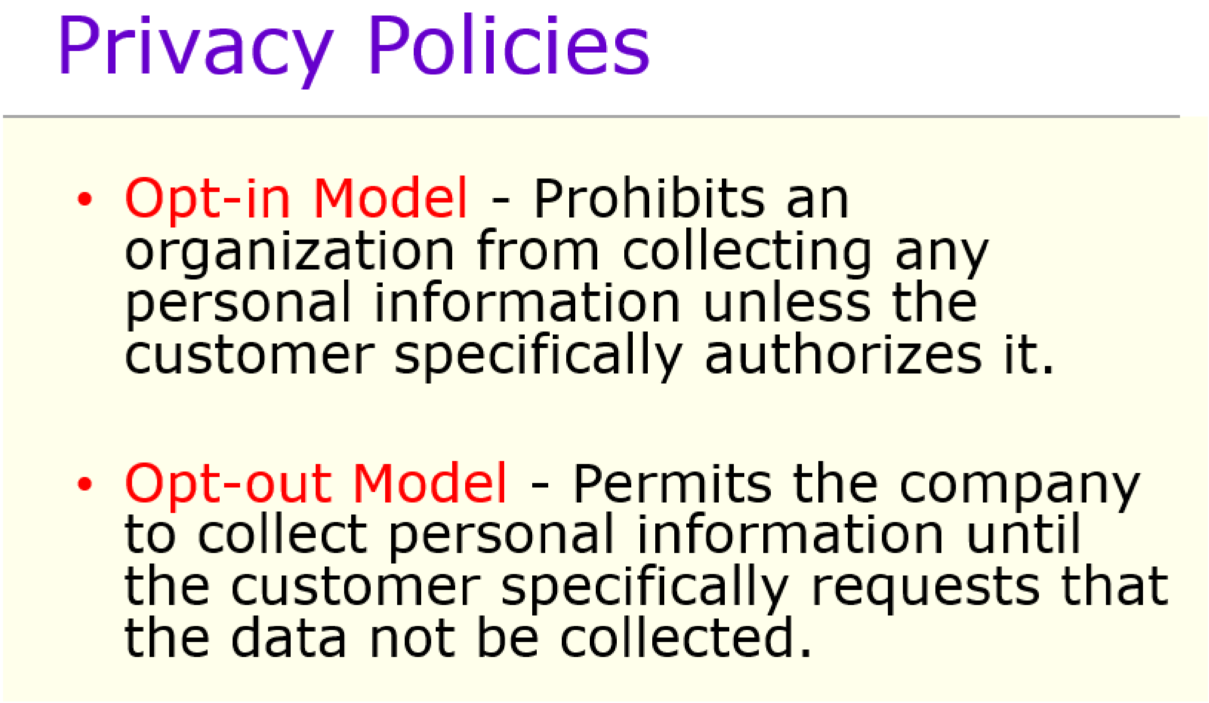
FIGURE 14.19

Key data privacy provisions of the agreement to protect the privacy of consumers in e-commerce transactions between the United States and the European Union.



U.S.–E.U. Data Privacy Requirements
• Notice of purpose and use of data collected
• Ability to opt out of third-party distribution of data
• Access for consumers to their information
• Adequate security, data integrity, and enforcement provisions

2. Describe Privacy Codes and Policies and its importance.



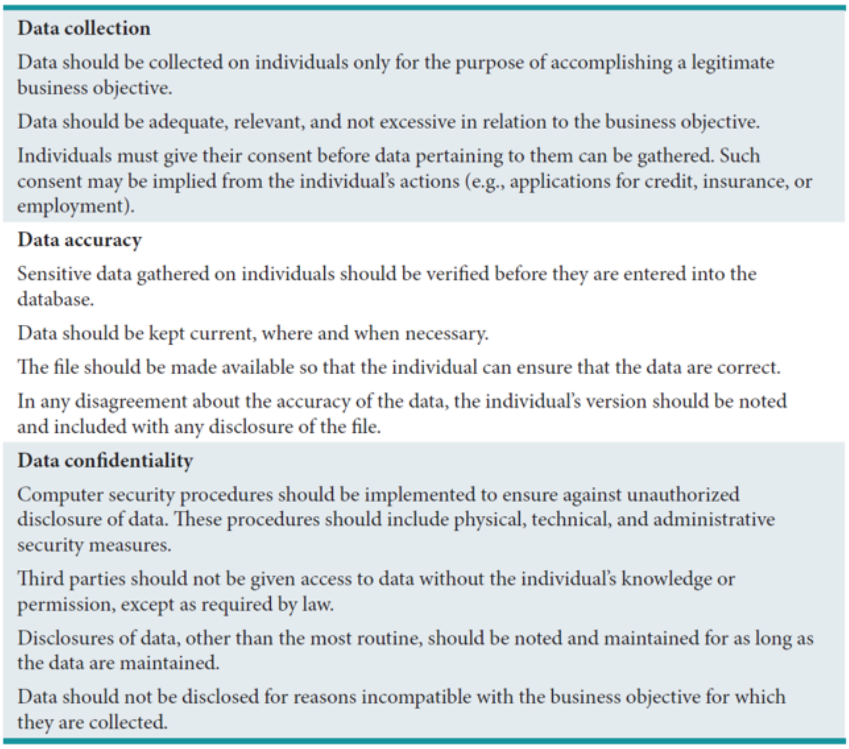
Privacy Policies

- Opt-in Model - Prohibits an organization from collecting any personal information unless the customer specifically authorizes it.
- Opt-out Model - Permits the company to collect personal information until the customer specifically requests that the data not be collected.

Privacy Policies (or Privacy Codes): an organization’s guidelines for protecting the privacy of its customers, clients, and employees.

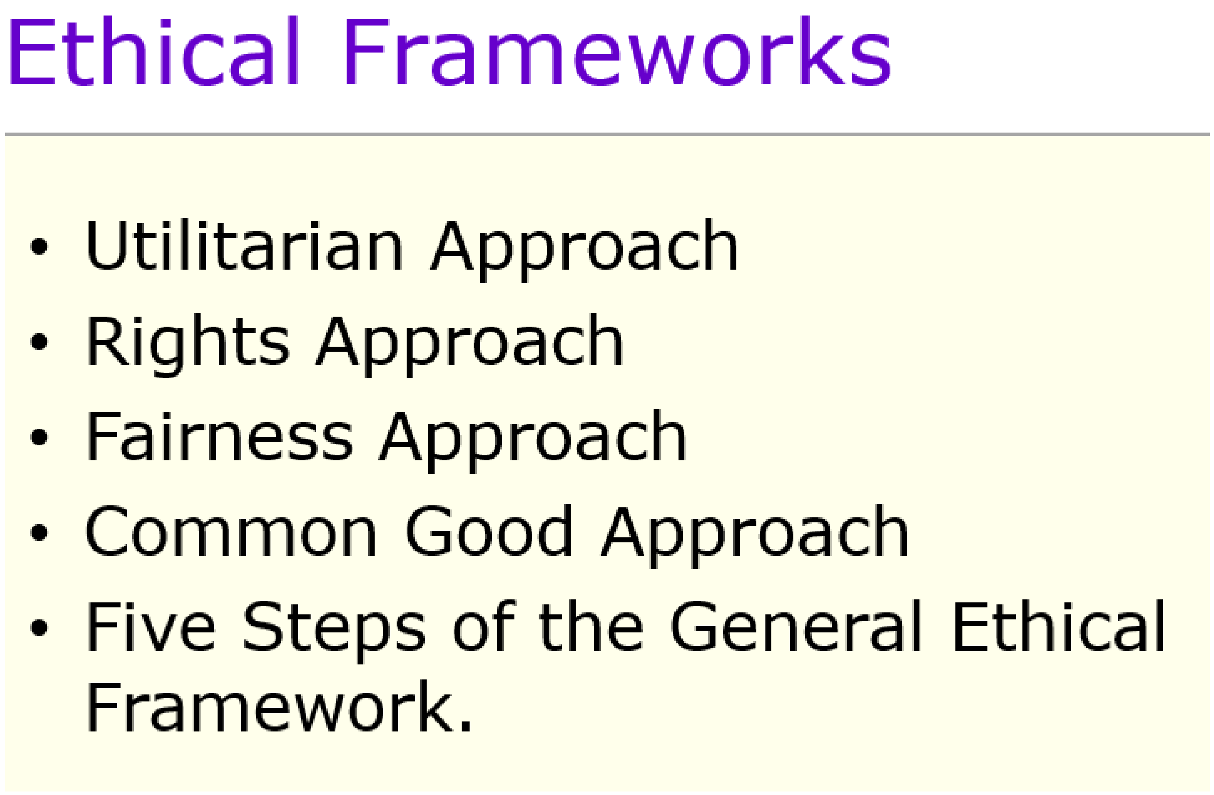
Opt-Out Model of Informed Consent: permits the company to collect personal information until the customer specifically requests that the data not be collected. Opt-In Model of Informed Consent: Prohibits an organization from collecting any personal information unless the customer specifically authorizes it.

Table 3.2: Privacy Policy Guidelines: A Sampler



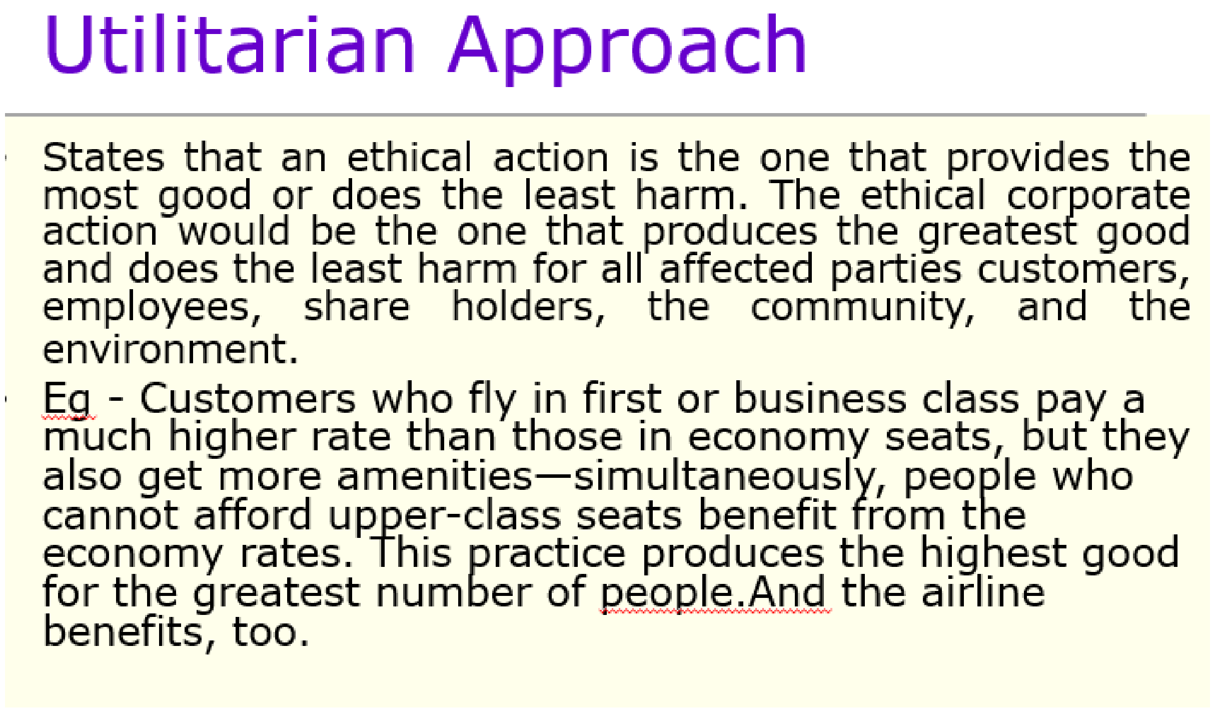
Data collection
Data should be collected on individuals only for the purpose of accomplishing a legitimate business objective.
Data should be adequate, relevant, and not excessive in relation to the business objective.
Individuals must give their consent before data pertaining to them can be gathered. Such consent may be implied from the individual's actions (e.g., applications for credit, insurance, or employment).
Data accuracy
Sensitive data gathered on individuals should be verified before they are entered into the database.
Data should be kept current, where and when necessary.
The file should be made available so that the individual can ensure that the data are correct.
In any disagreement about the accuracy of the data, the individual's version should be noted and included with any disclosure of the file.
Data confidentiality
Computer security procedures should be implemented to ensure against unauthorized disclosure of data. These procedures should include physical, technical, and administrative security measures.
Third parties should not be given access to data without the individual's knowledge or permission, except as required by law.
Disclosures of data, other than the most routine, should be noted and maintained for as long as the data are maintained.
Data should not be disclosed for reasons incompatible with the business objective for which they are collected.

3. Describe various ethical frameworks that can help us make ethical decisions.



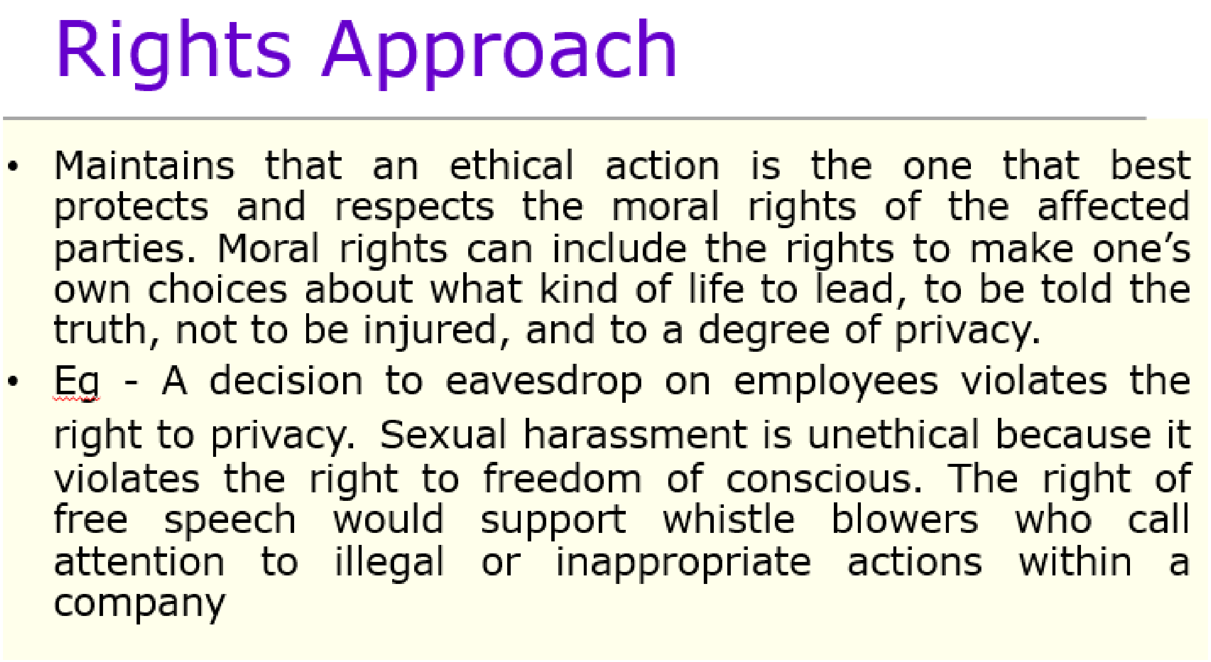
Ethical Frameworks

- Utilitarian Approach
- Rights Approach
- Fairness Approach
- Common Good Approach
- Five Steps of the General Ethical Framework.



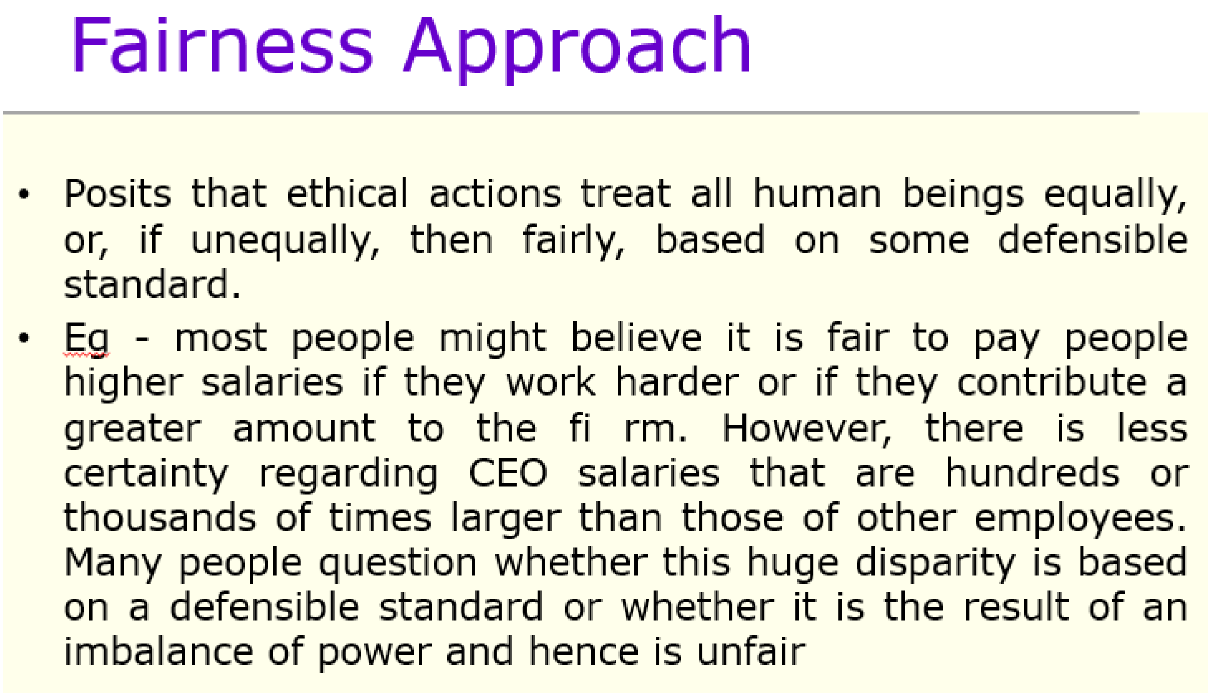
Utilitarian Approach

- States that an ethical action is the one that provides the most good or does the least harm. The ethical corporate action would be the one that produces the greatest good and does the least harm for all affected parties customers, employees, share holders, the community, and the environment.
- Eg - Customers who fly in first or business class pay a much higher rate than those in economy seats, but they also get more amenities—simultaneously, people who cannot afford upper-class seats benefit from the economy rates. This practice produces the highest good for the greatest number of people.And the airline benefits, too.



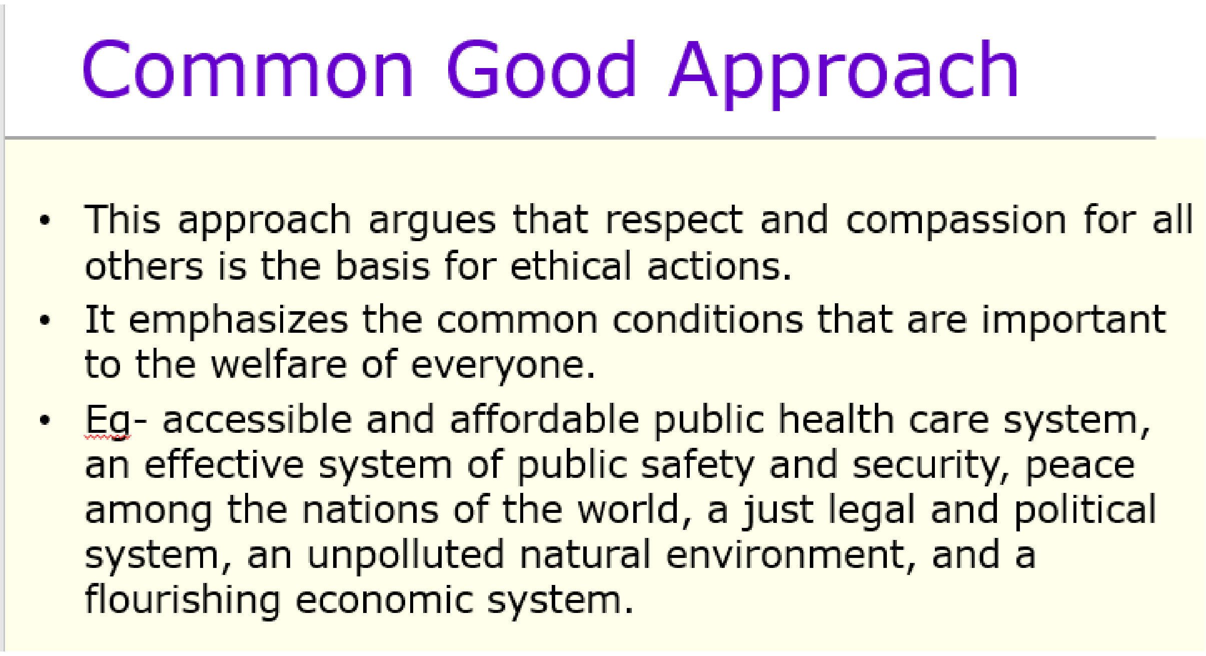
Rights Approach

- Maintains that an ethical action is the one that best protects and respects the moral rights of the affected parties. Moral rights can include the rights to make one’s own choices about what kind of life to lead, to be told the truth, not to be injured, and to a degree of privacy.
- Eg - A decision to eavesdrop on employees violates the right to privacy. Sexual harassment is unethical because it violates the right to freedom of conscious. The right of free speech would support whistle blowers who call attention to illegal or inappropriate actions within a company



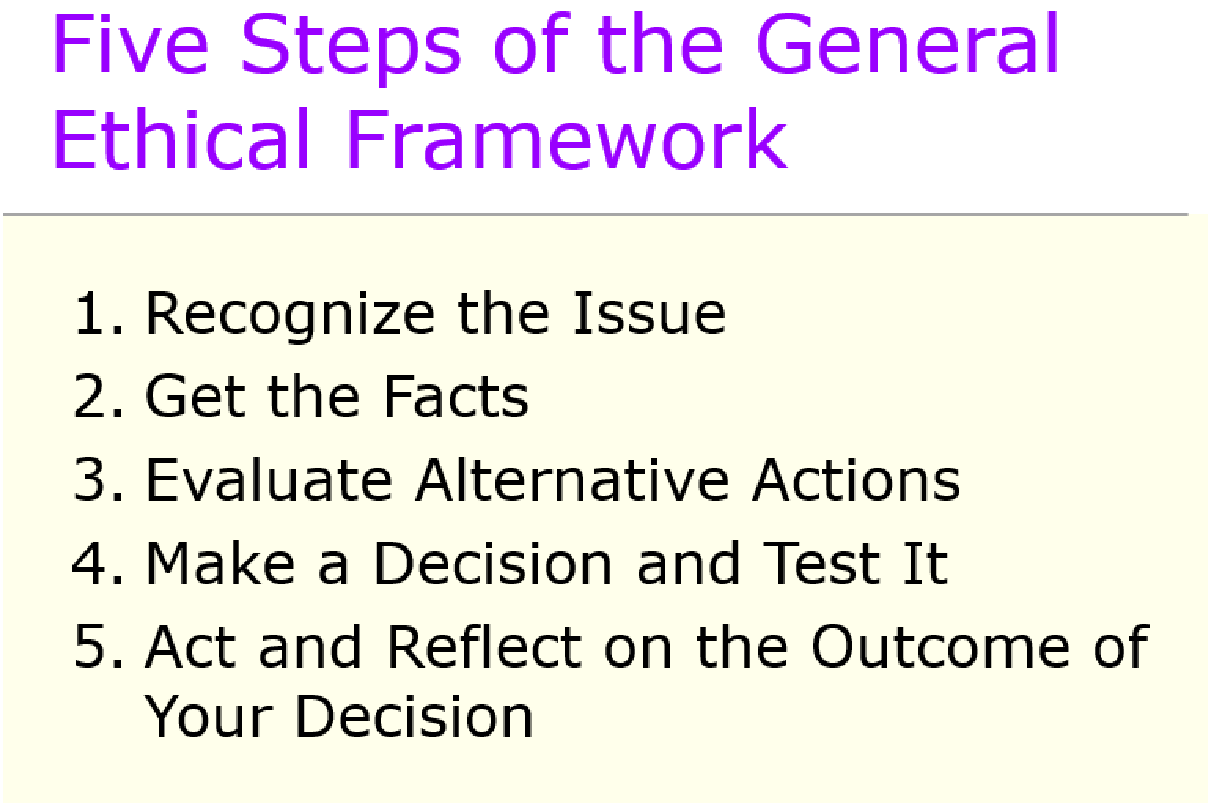
Fairness Approach

- Posits that ethical actions treat all human beings equally, or, if unequally, then fairly, based on some defensible standard.
- Eg - most people might believe it is fair to pay people higher salaries if they work harder or if they contribute a greater amount to the firm. However, there is less certainty regarding CEO salaries that are hundreds or thousands of times larger than those of other employees. Many people question whether this huge disparity is based on a defensible standard or whether it is the result of an imbalance of power and hence is unfair



Common Good Approach

- This approach argues that respect and compassion for all others is the basis for ethical actions.
- It emphasizes the common conditions that are important to the welfare of everyone.
- Eg- accessible and affordable public health care system, an effective system of public safety and security, peace among the nations of the world, a just legal and political system, an unpolluted natural environment, and a flourishing economic system.



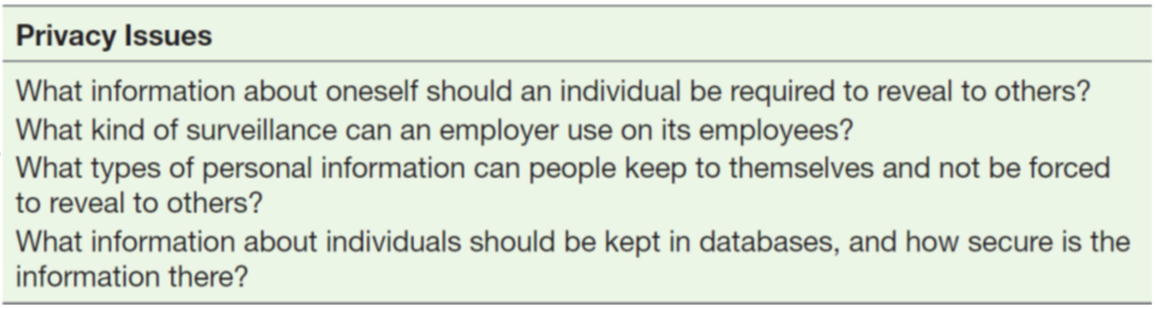
Five Steps of the General Ethical Framework

1. Recognize the Issue
2. Get the Facts
3. Evaluate Alternative Actions
4. Make a Decision and Test It
5. Act and Reflect on the Outcome of Your Decision

4. Describe the four categories of ethical issues related to information technology.

Ethics and Information Technology

- Privacy Issues: involve collecting, storing, and disseminating information about individuals
- Accuracy Issues: involve the authenticity, fidelity, and correctness of information that is collected and processed



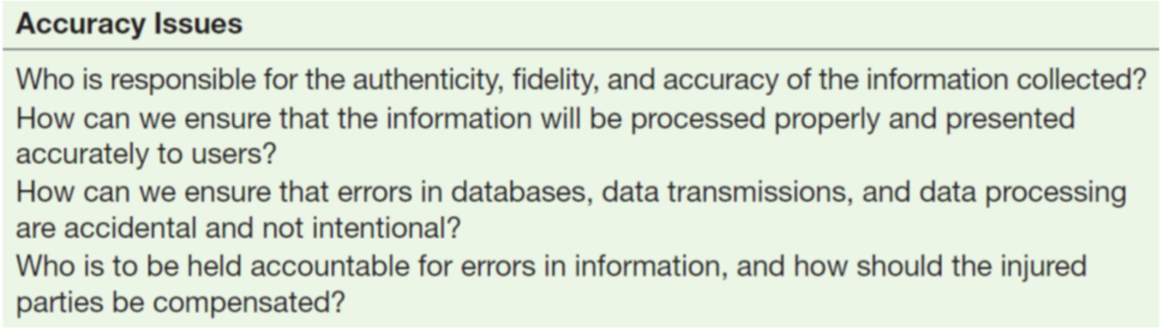
Privacy Issues

What information about oneself should an individual be required to reveal to others?

What kind of surveillance can an employer use on its employees?

What types of personal information can people keep to themselves and not be forced to reveal to others?

What information about individuals should be kept in databases, and how secure is the information there?



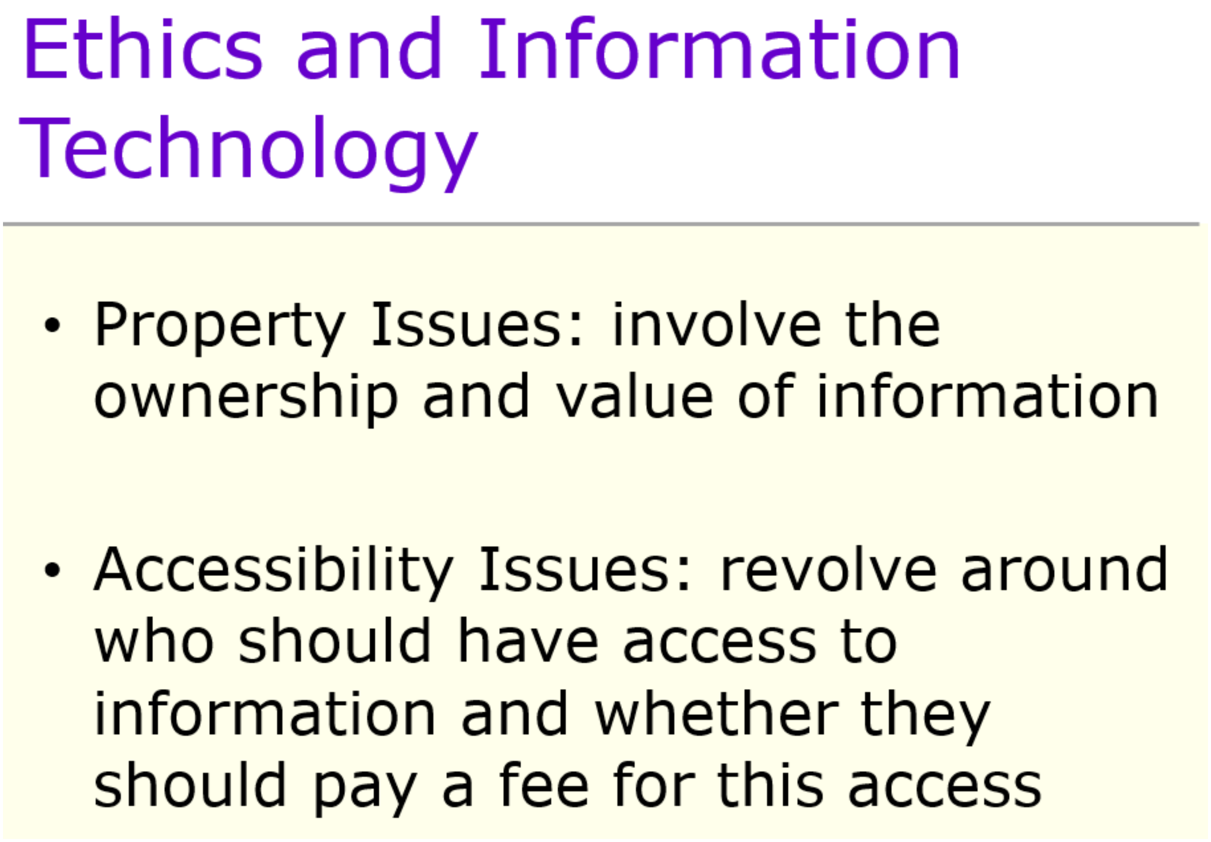
Accuracy Issues

Who is responsible for the authenticity, fidelity, and accuracy of the information collected?

How can we ensure that the information will be processed properly and presented accurately to users?

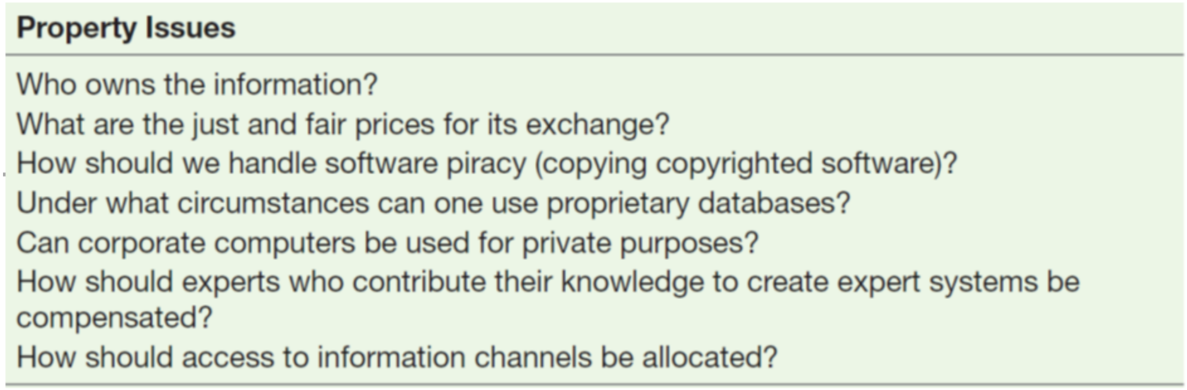
How can we ensure that errors in databases, data transmissions, and data processing are accidental and not intentional?

Who is to be held accountable for errors in information, and how should the injured parties be compensated?

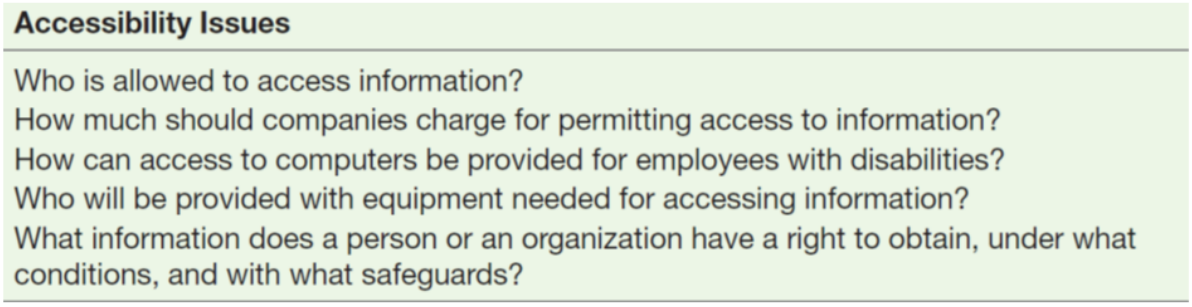


Ethics and Information Technology

- Property Issues: involve the ownership and value of information
- Accessibility Issues: revolve around who should have access to information and whether they should pay a fee for this access

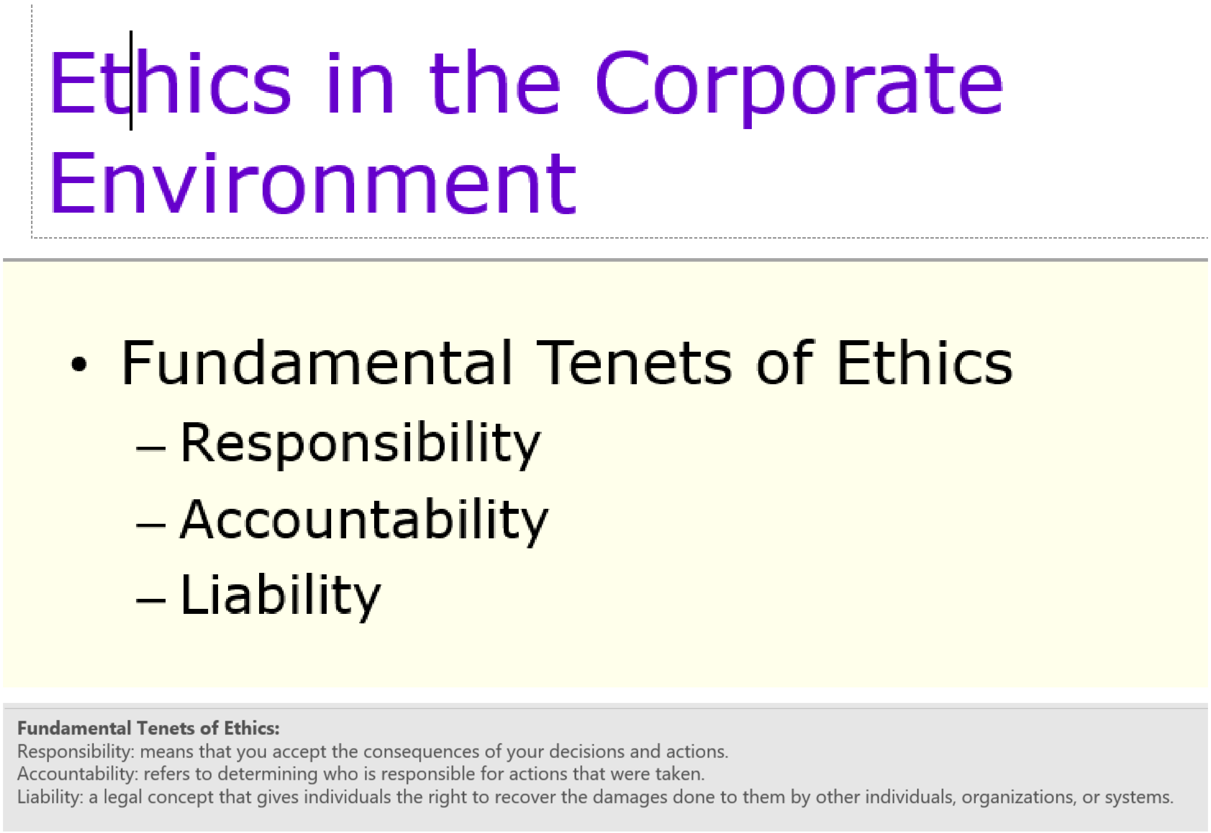


Property Issues
Who owns the information?
What are the just and fair prices for its exchange?
How should we handle software piracy (copying copyrighted software)?
Under what circumstances can one use proprietary databases?
Can corporate computers be used for private purposes?
How should experts who contribute their knowledge to create expert systems be compensated?
How should access to information channels be allocated?



Accessibility Issues
Who is allowed to access information?
How much should companies charge for permitting access to information?
How can access to computers be provided for employees with disabilities?
Who will be provided with equipment needed for accessing information?
What information does a person or an organization have a right to obtain, under what conditions, and with what safeguards?

5. List and describe the fundamental tenets of ethics.



Ethics in the Corporate Environment

- Fundamental Tenets of Ethics
  - Responsibility
  - Accountability
  - Liability

Fundamental Tenets of Ethics:
Responsibility: means that you accept the consequences of your decisions and actions.
Accountability: refers to determining who is responsible for actions that were taken.
Liability: a legal concept that gives individuals the right to recover the damages done to them by other individuals, organizations, or systems.

6. Identify three places that store personal data, and for each one, discuss at least one personal threat to the privacy of the data stored there.

Electronic Surveillance

Using technology to monitor individuals as they go about their daily routines.

Is conducted by employers, governments, and other institutions.

Examples:

Surveillance cameras in airports, subways, banks, and other public venues.

Electronic Surveillance

Inexpensive digital sensors are found in laptop webcams, video game sensors, smartphone cameras, utility meters, passports, and ID cards.

Smartphones create geotags

Google and Microsoft street view images

Satellite imaging

Personal Information in Databases

Personal Data / Record Keepers

Credit Reporting Agencies

Banks and Financial Institutions

Utility Companies

Employers

Hospitals

Schools

Government Agencies (IRS, State, City)

Personal Information in Databases

Major Concerns about Information You Provide Record Keepers

Do you know where the records are?

Are the records accurate?

Can you change inaccurate data?

How long will it take to make a change?

Under what circumstances will personal data be released?

Personal Information in Databases

Major Concerns about Information You Provide Record Keepers

How are the data used?

To whom are the data given or sold?

How secure are the data against access by unauthorized people?

Information on Internet Bulletin Boards, Newsgroups, and Social Networking Sites

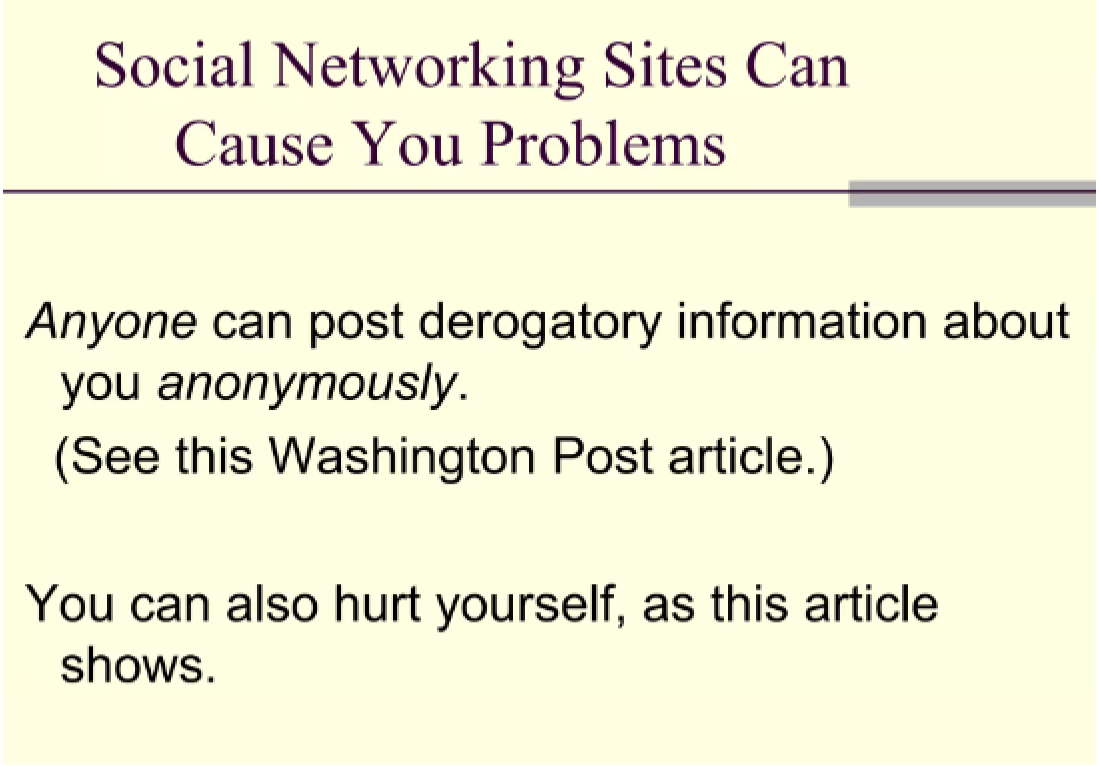
Free Speech versus Privacy on the Internet

Derogatory Information Can Influence Hiring Decisions

Little to No Recourse for Victims

3 places - information in databases, Internet bulletin boards, newsgroups, and social media sites. The privacy threat in Internet bulletin boards, newsgroups, and social

networking sites is that you might post personal information that many unknown people can see.



Social Networking Sites Can Cause You Problems

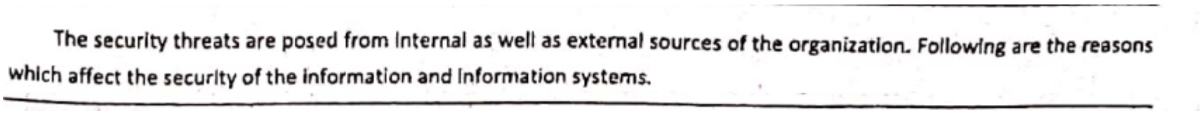
Anyone can post derogatory information about you *anonymously*.

(See this Washington Post article.)

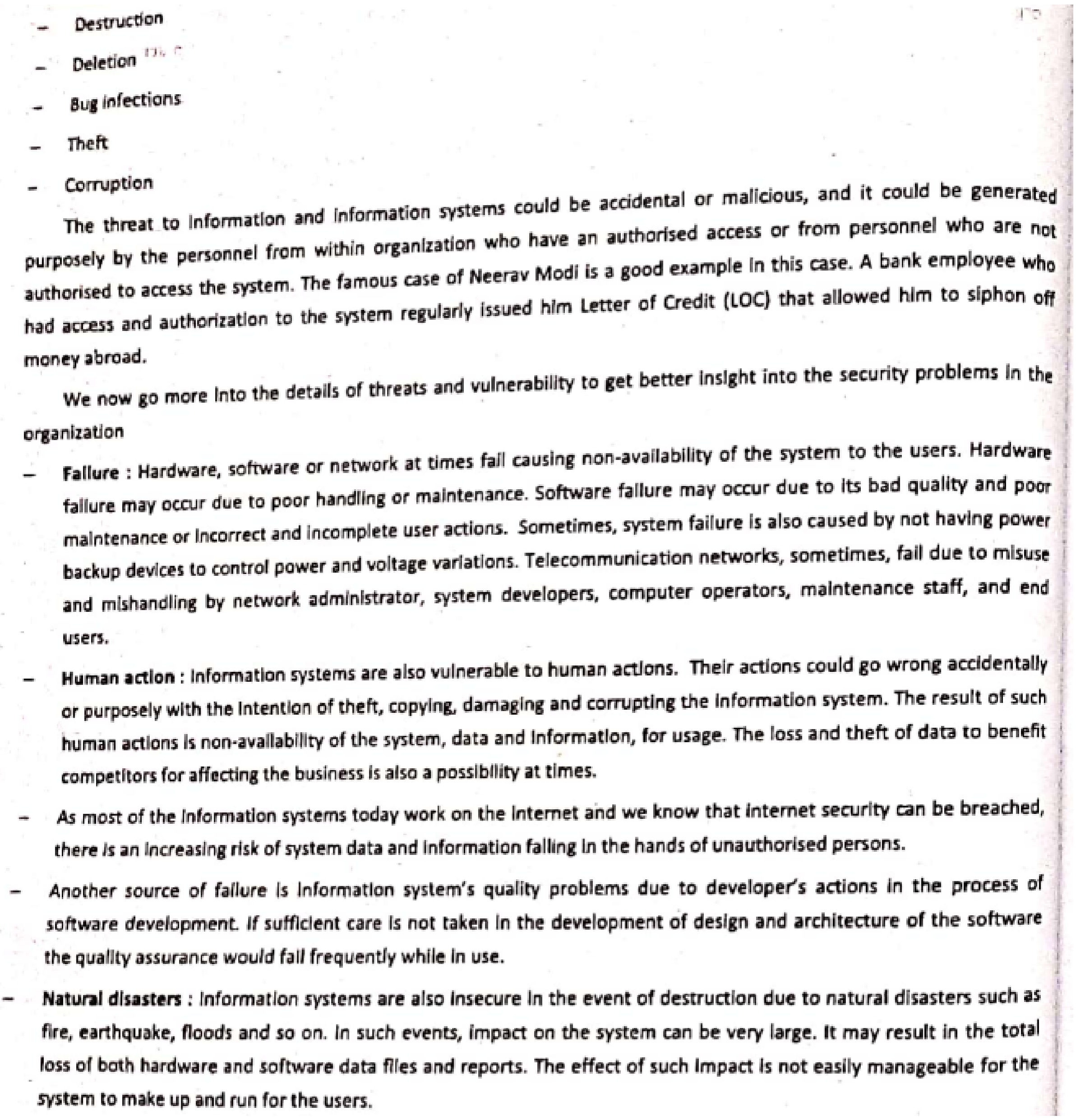
You can also hurt yourself, as this article shows.

7. Differentiate among a threat, an ex**posure, and a vulnerability.**

8. Explain the major threats to the Information systems.



The security threats are posed from internal as well as external sources of the organization. Following are the reasons which affect the security of the information and information systems.



- Destruction
- Deletion
- Bug infections
- Theft
- Corruption

The threat to information and information systems could be accidental or malicious, and it could be generated purposely by the personnel from within organization who have an authorised access or from personnel who are not authorised to access the system. The famous case of Neerav Modi is a good example in this case. A bank employee who had access and authorization to the system regularly issued him Letter of Credit (LOC) that allowed him to siphon off money abroad.

We now go more into the details of threats and vulnerability to get better insight into the security problems in the organization

- **Failure** : Hardware, software or network at times fail causing non-availability of the system to the users. Hardware failure may occur due to poor handling or maintenance. Software failure may occur due to its bad quality and poor maintenance or incorrect and incomplete user actions. Sometimes, system failure is also caused by not having power backup devices to control power and voltage variations. Telecommunication networks, sometimes, fail due to misuse and mishandling by network administrator, system developers, computer operators, maintenance staff, and end users.
- **Human action** : Information systems are also vulnerable to human actions. Their actions could go wrong accidentally or purposely with the intention of theft, copying, damaging and corrupting the information system. The result of such human actions is non-availability of the system, data and information, for usage. The loss and theft of data to benefit competitors for affecting the business is also a possibility at times.
- As most of the information systems today work on the internet and we know that internet security can be breached, there is an increasing risk of system data and information falling in the hands of unauthorised persons.
- Another source of failure is information system's quality problems due to developer's actions in the process of software development. If sufficient care is not taken in the development of design and architecture of the software the quality assurance would fail frequently while in use.
- **Natural disasters** : Information systems are also insecure in the event of destruction due to natural disasters such as fire, earthquake, floods and so on. In such events, impact on the system can be very large. It may result in the total loss of both hardware and software data files and reports. The effect of such impact is not easily manageable for the system to make up and run for the users.

9. Describe various Unintentional threats.

- **Unintentional, insider-originated security breaches are the result of simple negligence, inattention, or lack of education. Unintentional mistakes such as a system administrator errors, operator errors and programming errors for example, are common.**
- **Unintentional, innocent, or negligent technical threats include software bugs that occur during the programming of a computer system, and system configuration errors, such as the use of improper settings or parameters when software is installed.**

10. Describe various Intentional threats.

- **Intentional acts can be overt and direct action (e.g. when an employee with access to customer credit card information sells it to third party) or can be from individuals who use covert technical means.**
- **Intentional and malicious technical threats that typically involve the use of computer code or other technical devices designated to cause trouble. This includes: software bugs intentionally added to computer programs, malicious software that modifies or destroys data – such as viruses, worms, and Trojan horses, back doors that allow unauthorized access to a system, eavesdropping programs designed to copy and transmit communications or other information, network spoofing, denial of service attacks, password cracking, email hijacking, packet replay and packet modification.**

11. What are the different types of software attacks?

Malware Attack

This is one of the most common types of cyberattacks. “Malware” refers to malicious software viruses including worms, spyware, ransomware, adware, and trojans. Malware breaches a network through a vulnerability. When the user clicks a dangerous link, it downloads an email attachment or when an infected pen drive is used.

Phishing Attack
Phishing attacks are one of the most prominent widespread types of cyberattacks. It is a type of social engineering attack wherein an attacker impersonates to be a trusted contact and sends the victim fake mails.

Unaware of this, the victim opens the mail and clicks on the malicious link or opens the mail's attachment. By doing so, attackers gain access to confidential information and account credentials. They can also install malware through a phishing attack.
Password Attack
It is a form of attack wherein a hacker cracks your password with various programs and password cracking tools like Aircrack, Cain, Abel, John the Ripper, Hashcat, etc. There are different types of password attacks like brute force attacks, dictionary attacks, and keylogger attacks.
Man-in-the-Middle Attack
A Man-in-the-Middle Attack (MITM) is also known as an eavesdropping attack. In this attack, an attacker comes in between a two-party communication, i.e., the attacker hijacks the session between a client and host. By doing so, hackers steal and manipulate data.

As seen below, the client-server communication has been cut off, and instead, the communication line goes through the hacker.

SQL Injection Attack

A Structured Query Language (SQL) injection attack occurs on a database-driven website when the hacker manipulates a standard SQL query. It is carried by injecting a malicious code into a vulnerable website search box, thereby making the server reveal crucial information.

This results in the attacker being able to view, edit, and delete tables in the databases. Attackers can also get administrative rights through this.

Denial-of-Service Attack

A Denial-of-Service Attack is a significant threat to companies. Here, attackers target systems, servers, or networks and flood them with traffic to exhaust their resources and bandwidth.

When this happens, catering to the incoming requests becomes overwhelming for the servers, resulting in the website it hosts either shut down or slow down. This leaves the legitimate service requests unattended.

It is also known as a DDoS (Distributed Denial-of-Service) attack when attackers use multiple compromised systems to launch this attack.

Insider Threat

As the name suggests, an insider threat does not involve a third party but an insider. In such a case; it could be an individual from within the organization who knows everything about the organization. Insider threats have the potential to cause tremendous damages.

Insider threats are rampant in small businesses, as the staff there hold access to multiple accounts with data. Reasons for this form of an attack are many, it can be greed, malice, or even carelessness. Insider threats are hard to predict and hence tricky.

12. What is a SCADA system?

A SCADA system is a combination of hardware and software that enables the automation of industrial processes by capturing Operational Technology (OT) real-time data. SCADA connects the sensors that monitor equipment like motors, pumps, and valves to an onsite or remote server.

A SCADA system empowers organizations to:

- Control processes locally or at remote locations
- Acquire, analyze and display real-time data
- Directly interact with industrial equipment such as sensors, valves, pumps, and motors
- Record and archive events for future reference or report creation.

SCADA system hardware

Hardware such as Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs) serve as local collection points for acquiring sensor information. This hardware in a modern SCADA system will often trigger actions of the connected piece of equipment via programmed logic. In a SCADA system, the collected data from the sensors is gathered by a computer commonly known as a “gateway.”

Different edge workloads use computer hardware in various ways.

- **Gateways** pass the data from PLCs to servers or to the edge.
- **Edge computers** are close to the source of the data and can act as a gateway. However, they will first process the data before transferring to the cloud or central physical server. This enables quicker decisions at a local level as well as bandwidth and cost savings.
- **Human Machine Interfaces (HMIs)** provide a local touchscreen interface for machine monitoring and control. They can also act as gateways or edge computers.
- **The server itself** acts as the central control for your local SCADA system. Your local historian server (historical data logging over time) may live here. Depending on the architecture it may also report back to cloud or a larger server on the enterprise network

Once collected, sensor data can either be acted upon directly through the use of SCADA software, or saved for later review. SCADA systems can help monitor and control processes from the same location in which actions are performed, or from a remote site.

13. Explain risk management in protecting information resources?

A risk is the probability that a threat will impact an information resource. The goal of risk management is to identify, control, and minimize the impact of threats. In other words, risk management seeks to reduce risk to acceptable levels. Risk management consists of three processes: risk analysis, risk mitigation, and controls evaluation. Organizations perform risk analyses to ensure that their IS security programs are cost effective. Risk analysis involves three steps: (1) assessing the value of each asset being protected, (2) estimating the probability that each asset will be compromised, and (3) comparing the probable costs of the asset’s being compromised with the costs of protecting that asset. The organization then considers how to mitigate the risk. In risk mitigation, the organization takes concrete actions against risks. Risk mitigation has two functions: (1) implementing controls to prevent identified threats from occurring, and (2) developing a means of recovery if the threat becomes a reality. There are several risk mitigation strategies that organizations can adopt. The three most common are risk acceptance, risk limitation, and risk transference.

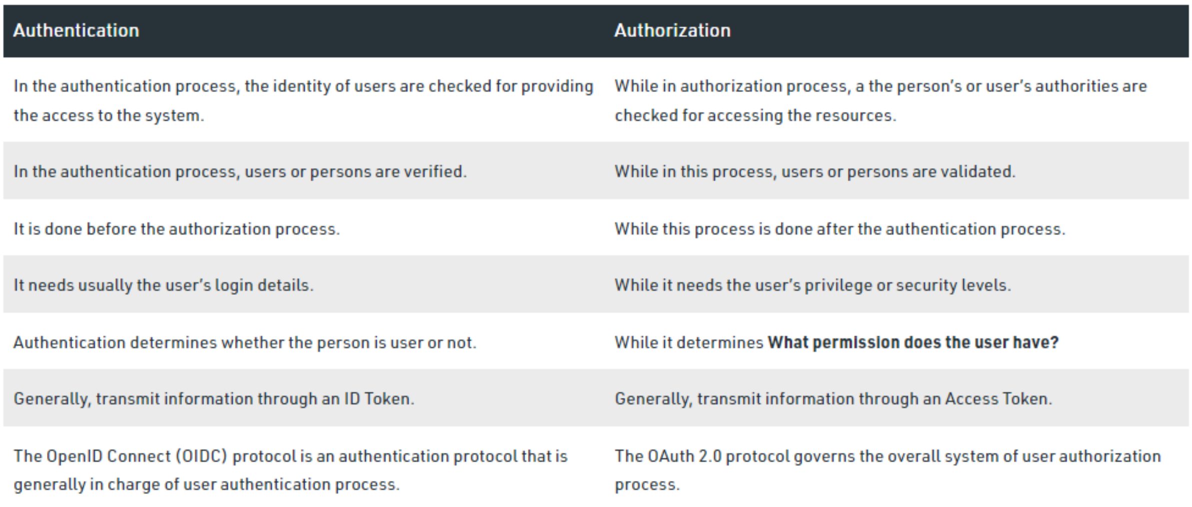
Risk acceptance: Accept the potential risk, continue operating with no controls, and absorb any damages that occur.

• Risk limitation: Limit the risk by implementing controls that minimize the impact of the threat.

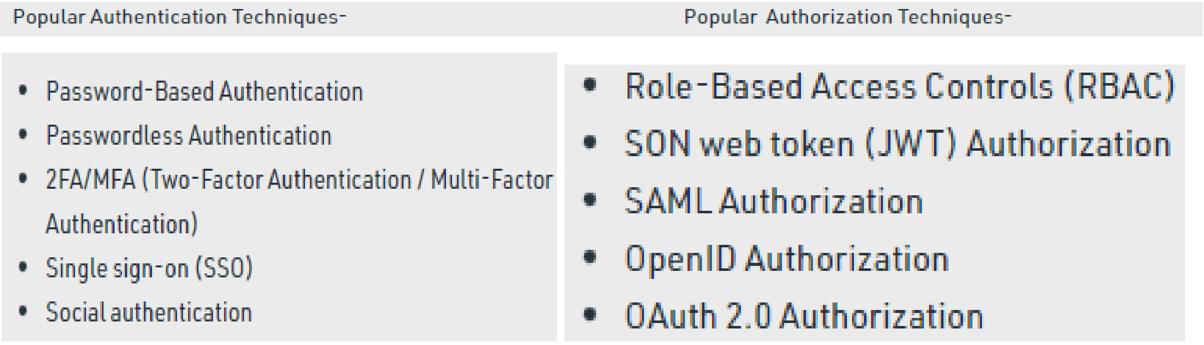
• Risk transference: Transfer the risk by using other means to compensate for the loss, such as by purchasing insurance.

Finally, in controls evaluation, the organization examines the costs of implementing adequate control measures against the value of those control measures. If the costs of implementing a control are greater than the value of the asset being protected, the control is not cost effective. In the next section, you will study the various controls that organizations use to protect their information resources.

14. Differentiate between authentication and authorization. Which one of these always performed first?



Authentication	Authorization
In the authentication process, the identity of users are checked for providing the access to the system.	While in authorization process, a the person's or user's authorities are checked for accessing the resources.
In the authentication process, users or persons are verified.	While in this process, users or persons are validated.
It is done before the authorization process.	While this process is done after the authentication process.
It needs usually the user's login details.	While it needs the user's privilege or security levels.
Authentication determines whether the person is user or not.	While it determines **What permission does the user have?**
Generally, transmit information through an ID Token.	Generally, transmit information through an Access Token.
The OpenID Connect (OIDC) protocol is an authentication protocol that is generally in charge of user authentication process.	The OAuth 2.0 protocol governs the overall system of user authorization process.

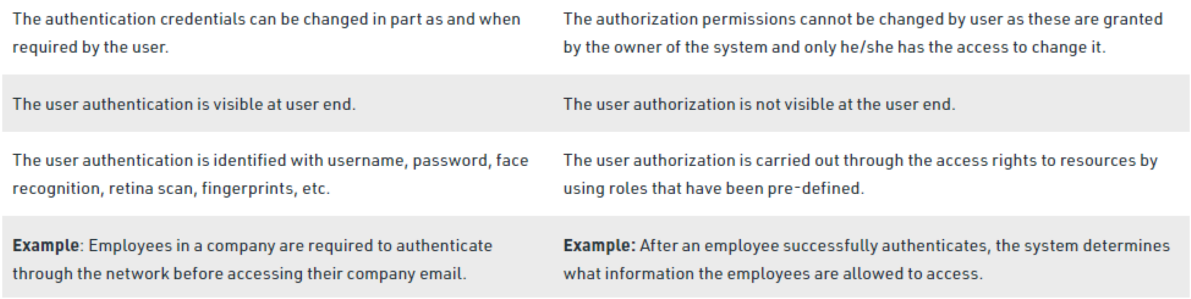


Popular Authentication Techniques-

- Password-Based Authentication
- Passwordless Authentication
- 2FA/MFA (Two-Factor Authentication / Multi-Factor Authentication)
- Single sign-on (SSO)
- Social authentication

Popular Authorization Techniques-

- Role-Based Access Controls (RBAC)
- SON web token (JWT) Authorization
- SAML Authorization
- OpenID Authorization
- OAuth 2.0 Authorization



The authentication credentials can be changed in part as and when required by the user.	The authorization permissions cannot be changed by user as these are granted by the owner of the system and only he/she has the access to change it.
The user authentication is visible at user end.	The user authorization is not visible at the user end.
The user authentication is identified with username, password, face recognition, retina scan, fingerprints, etc.	The user authorization is carried out through the access rights to resources by using roles that have been pre-defined.
Example: Employees in a company are required to authenticate through the network before accessing their company email.	**Example:** After an employee successfully authenticates, the system determines what information the employees are allowed to access.

15. Explain any two communications controls used for information system security.

Communications controls (also called network controls) secure the movement of data across networks. Communications controls consist of firewalls, antimalware systems, whitelisting and blacklisting, encryption, virtual private networks (VPNs), secure socket layer (SSL), and employee monitoring systems.

Firewalls

A firewall is a system that prevents a specific type of information from moving between untrusted networks, such as the Internet, and private networks, such as your company's network.

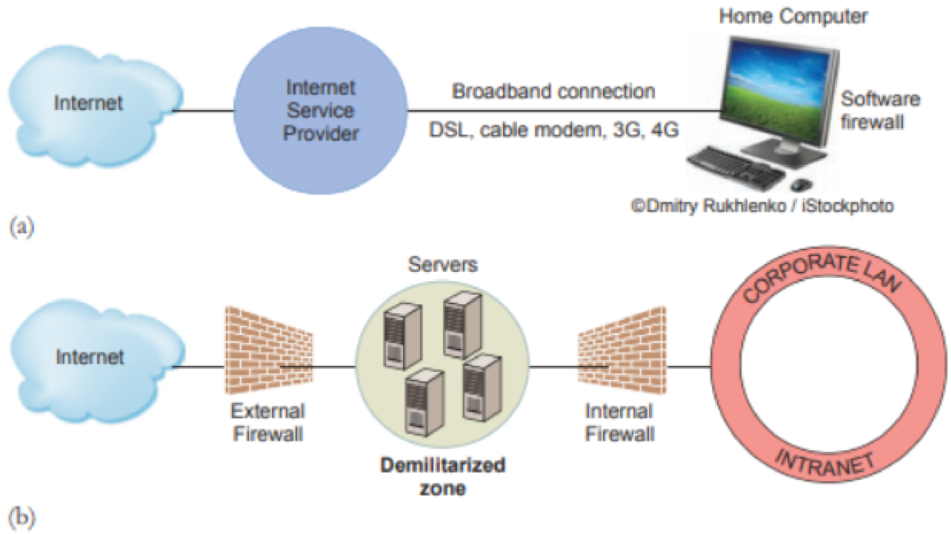
Simply, firewalls prevent unauthorized Internet users from accessing private networks. All messages entering or leaving your company's network pass through a firewall.

The firewall examines each message and blocks those that do not meet specified security rules.

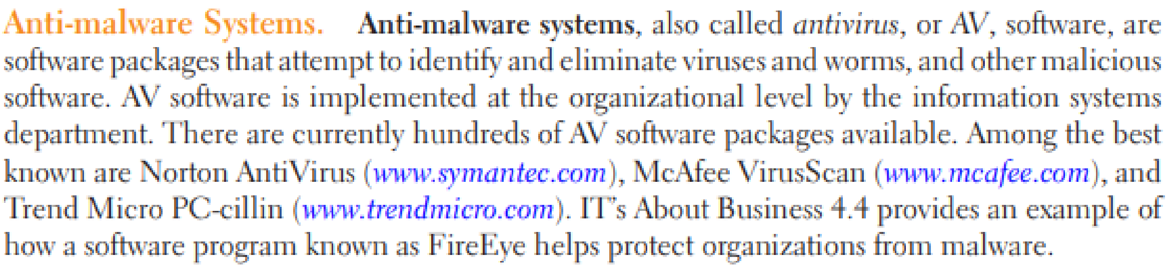
Firewalls range from simple, for home use, to very complex for organizational use. Figure (a) illustrates a basic firewall for a home computer. In this case, the firewall is implemented as software on the home computer.

Figure (b) shows an organization that has implemented an external firewall, which faces the Internet, and an internal firewall, which faces the company network. Corporate firewalls typically consist of software running on a computer dedicated to the task.

A demilitarized zone (DMZ) is located between the two firewalls. Messages from the Internet must first pass through the external firewall. If they conform to the defined security rules, they are then sent to company servers located in the DMZ.



a) Basic firewall for home computer b) Organization with two firewalls and demilitarized zone


Anti-malware Systems. **Anti-malware systems**, also called *antivirus*, or AV, software, are software packages that attempt to identify and eliminate viruses and worms, and other malicious software. AV software is implemented at the organizational level by the information systems department. There are currently hundreds of AV software packages available. Among the best known are Norton AntiVirus (*www.symantec.com*), McAfee VirusScan (*www.mcafee.com*), and Trend Micro PC-cillin (*www.trendmicro.com*). IT's About Business 4.4 provides an example of how a software program known as FireEye helps protect organizations from malware.

Whitelisting and Blacklisting

Whitelisting permits acceptable software to run, and it either prevents any other software from running or it lets new software run in a quarantined environment until the company can verify its validity.

Whereas whitelisting allows nothing to run unless it is on the whitelist, blacklisting allows everything to run unless it is on the blacklist.

A blacklist, then, includes certain types of software that are not allowed to run in the company environment.

For example, a company might blacklist peer-to-peer file sharing on its systems. In addition to software, people, devices, and Web sites can also be whitelisted and blacklisted.