Ethics and Privacy, Information Security

Ethics refers to the principles of right and wrong that individuals use to make choices that guide their behavior. Deciding what is right or wrong is not always easy or clear-cut. Fortunately, there are many frameworks that can help us make ethical decisions.

Most widely used Ethical Standards (Imp)

- The ***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, shareholders, the community, and the physical environment.
- The ***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 enjoy a degree of privacy. Which of these rights people are actually entitled to—and under what circumstances— is widely debated. Nevertheless, most people acknowledge that individuals are entitled to some moral rights (woman's rights, children rights, SC/ST, underprivileged). An ethical organizational action would be one that protects and respects the moral rights of customers, employees, shareholders, business partners, and even competitors.
- The ***fairness approach*** posits that ethical actions treat all human beings equally, or, if unequally, then fairly, based on some defensible standard. For example, 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 fi rm. 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.
- Finally, **the *common good approach*** highlights the interlocking relationships that underlie all societies. 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. These conditions can include a system of laws, effective police and fire departments, healthcare, a public educational system, and even public recreation areas. We pay taxes though government misuse the money we pay many times because it is used for the above causes also.

Explain Ethical Frameworks: (The above standards are used for frameworks – Mention them)

If we combine these four standards, we can develop a **general framework for ethics (or ethical decision making**). This framework consists of five steps:

- Recognize an ethical issue:
  - Could this decision or situation damage someone or some group?
  - Does this decision involve a choice between a good and a bad alternative?
  - Does this issue involve more than simply legal considerations? If so, then in what way?
- Get the facts:
  - What are the relevant facts of the situation?

º Do I have sufficient information to make a decision?
º Which individuals and/or groups have an important stake in the outcome?
º Have I consulted all relevant persons and groups?

- Evaluate alternative actions:
  º Which option will produce the most good and do the least harm? (the utilitarian approach)
  º Which option best respects the rights of all stakeholders? (the rights approach)
  º Which option treats people equally or proportionately? (the fairness approach)
  º Which option best serves the community as a whole, and not just some members? (the common good approach)
- Make a decision and test it:
  º Considering all the approaches, which option best addresses the situation?
- Act and reflect on the outcome of your decision:
  º How can I implement my decision with the greatest care and attention to the concerns of all stakeholders?
  º How did my decision turn out, and what did I learn from this specific situation?

What are the Fundamental tenets of ethics?

Fundamental tenets of ethics include responsibility, accountability, and liability:

- **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** is a legal concept that gives individuals the right to recover the damages done to them by other individuals, organizations, or systems.

What is *unethical* is not necessarily *illegal*. Explain the statement with an example.

It is critical that we realize that what is *unethical* is not necessarily *illegal*.
For example, a bank's decision to foreclose on a home (for non-repayment of loans) can be technically legal, but it can raise many ethical questions. In many instances, then, an individual or organization faced with an ethical decision is not considering whether to break the law. As the foreclosure example illustrates, however, ethical decisions can have serious consequences for individuals, organizations, and society at large.
We have witnessed many extremely poor ethical decisions, not to mention outright criminal behavior, at many organizations. At each company, executives were convicted of various types of fraud for using illegal accounting practices.

Advancements in information technologies have generated a new set of ethical problems. Justify

1. Regarding Data:

- Organizations to collect, integrate, and distribute enormous amounts of information on individuals, Groups, and institutions. These developments have created numerous ethical problems concerning the appropriate collection and use of customer information, personal privacy, and the protection of intellectual property.
- Sale of data to marketing firms

- These developments affect the academic world as well. For example, vast amounts of information on the Internet make it easier for students to **plagiarize** papers and essays.

2. Other Corporate Issues in Ethics:
Many of the business decisions you will face at work will have an ethical dimension. Consider the following decisions that you might have to make:

- Should organizations monitor employees' Web surfing and e-mail?
- Should organizations sell customer information to other companies?
- Should organizations audit employees' computers for unauthorized software or illegally downloaded music or video files?

3. The diversity and ever-expanding use of IT applications have created a variety of ethical issues. These issues fall into four general categories: **privacy, accuracy, property, and accessibility.**

- *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.
- *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.

Ethics in the Corporate Environment

Many companies and professional organizations develop their own codes of ethics. A **code of ethics** is a collection of principles intended to guide decision making by members of the organization. For example, the Association for Computing Machinery (*www.acm.org*), an organization of computing professionals, has a thoughtful code of ethics for its members. The Google Code of Conduct is one of the ways they put Google's values into practice. It's built around the recognition that everything the employees do in connection with work at Google will be, and should be, measured against the highest possible standards of ethical business conduct.

(You can mention the points in the previous 3 questions also – from tenets of ethics)

Describe the issue of privacy as it is affected by IT.

- In general, **privacy** is the right to be left alone and to be free of unreasonable personal intrusions. **Information privacy** is the right to determine when, and to what extent, information about you can be gathered and/or communicated to others.
- Privacy rights apply to individuals, groups, and institutions. The right to privacy is recognized today in all the states and by the government, either by statute or in common law.
- Privacy can be interpreted quite broadly. However, court decisions in many countries have followed two rules fairly closely:
  1. The right of privacy is not absolute. Privacy must be balanced against the needs of society.
  2. The public's right to know supersedes the individual's right of privacy.

(Important) Rapid advances in information technologies have made it much easier to collect, store, and integrate vast amounts of data on individuals in large databases. On an average day, data about you are generated in many ways: surveillance cameras located on toll roads, on other roadways, in busy intersections, in public places, and at work; credit card Transactions; telephone calls (landline and cellular); banking transactions; queries to search engines; and government records (including police records). These data can be integrated to produce a **digital dossier**, which is an electronic profile of you and your habits. The process of forming a digital dossier is called **profiling**.

Data aggregators, such as LexisNexis (*www.lexisnexis.com*), ChoicePoint (*www.choicepoint.com*), and Acxiom (*www.acxiom.com*), are prominent examples of profilers. These companies collect public data such as real estate records and published telephone numbers, in addition to non-public information such as Social Security numbers; financial data; and police, criminal, and motor vehicle records. They then integrate these data to form digital dossiers and sell them to companies that want to know their customers better, a process called ***customer intimacy*.**

Electronic Surveillance

- According to the American Civil Liberties Union (ACLU), tracking people's activities with the aid of information technology has become a major privacy-related problem. The ACLU notes that this monitoring, or **electronic surveillance**, is rapidly increasing, particularly with the emergence of new technologies. Electronic surveillance is conducted by employers, the government, and other institutions.
- Surveillance cameras track you at airports, subways, banks, and other public venues. In addition, inexpensive digital sensors are now everywhere. They are incorporated into laptop webcams, video-game motion sensors, smartphone cameras, utility meters, passports, and employee ID cards.
- Emerging technologies such as low-cost digital cameras, motion sensors, and biometric readers are helping to increase the monitoring of human activity. In addition, the costs of storing and using digital data are rapidly decreasing. The result is an explosion of sensor data collection and storage.
- Another example of how new devices can contribute to electronic surveillance is facial recognition technology. Google and Facebook are using facial-recognition software—Google Picasa and Facebook Photo Albums—in their popular online photo-editing and sharing services. Both companies encourage users to assign names to people in photos, a practice referred to as ***photo tagging***.

Personal Information in Databases

Modern institutions store information about individuals in many databases. Example: credit-reporting agencies. Other institutions that store personal information include banks and financial institutions; cable TV, telephone, and utilities companies; employers; mortgage companies; hospitals; schools and universities; retail establishments; government agencies (Internal Revenue Service, your state, your municipality); and many others.

There are several concerns about the information you provide to these record keepers. Some of the major concerns are as follows:

- 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 the personal data be released?
- 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

Every day we see more and more *electronic bulletin boards*, *newsgroups*, *electronic discussions* such as chat rooms, and *social networking sites*. These sites appear on the Internet, within corporate intranets, and on blogs. A *blog*, short for “Weblog,” is an informal, personal journal that is frequently updated and is intended for general public reading. YouTube videos are another cause of concern.

How does society keep owners of bulletin boards/YouTube/ Social networking sites from disseminating information that may be offensive to readers or simply untrue?

How organizations can ensure Privacy Codes and Policies of customers?

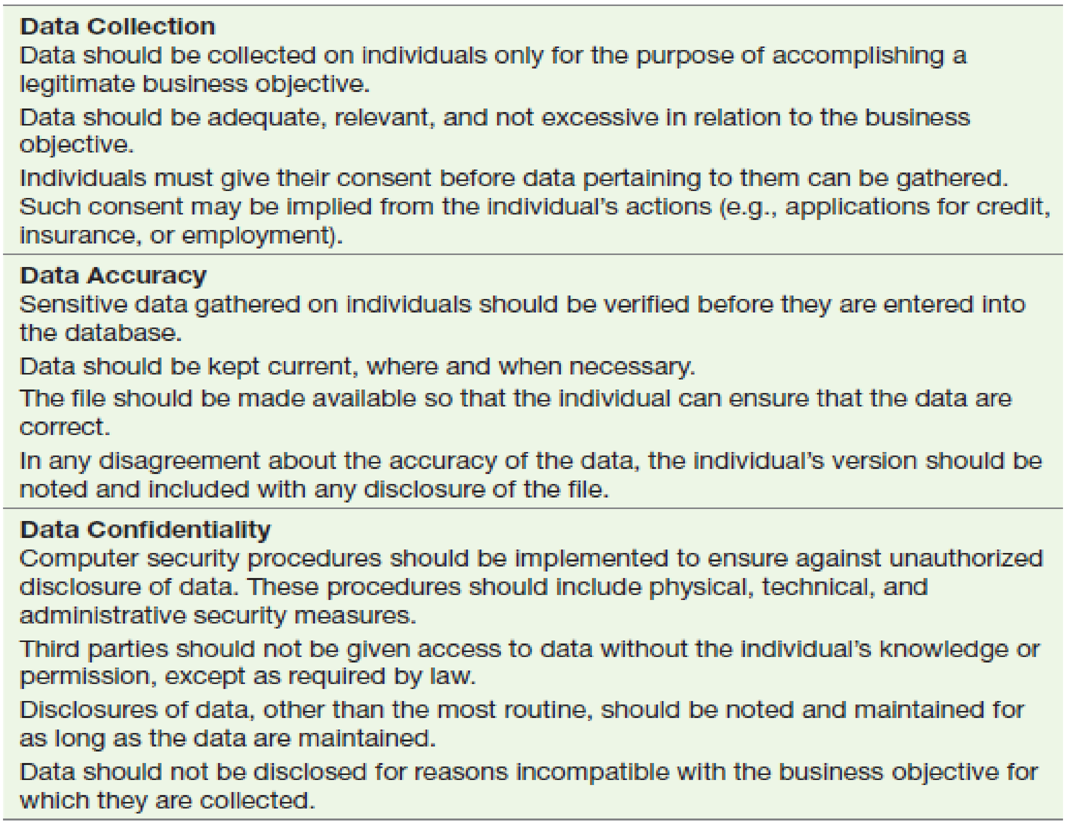
Privacy policies or **privacy codes** are an organization’s guidelines for protecting the privacy of its customers, clients, and employees. In many corporations, management has begun to understand that when they collect vast amounts of personal information, they must protect it. In addition, many organizations give their customers some voice in how their information is used by providing them with opt-out choices.

✓ The **opt-out model** of informed consent permits the company to collect personal information until the customer specifically requests that the data not be collected.

✓ Privacy advocates prefer the **opt-in model** of informed consent, which prohibits an organization from collecting any personal information unless the customer specifically authorizes it.

✓

Privacy Policy Guidelines: A Sample



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.

Discuss how privacy issues can impact transborder data flows./ What are the International Aspects of Privacy.

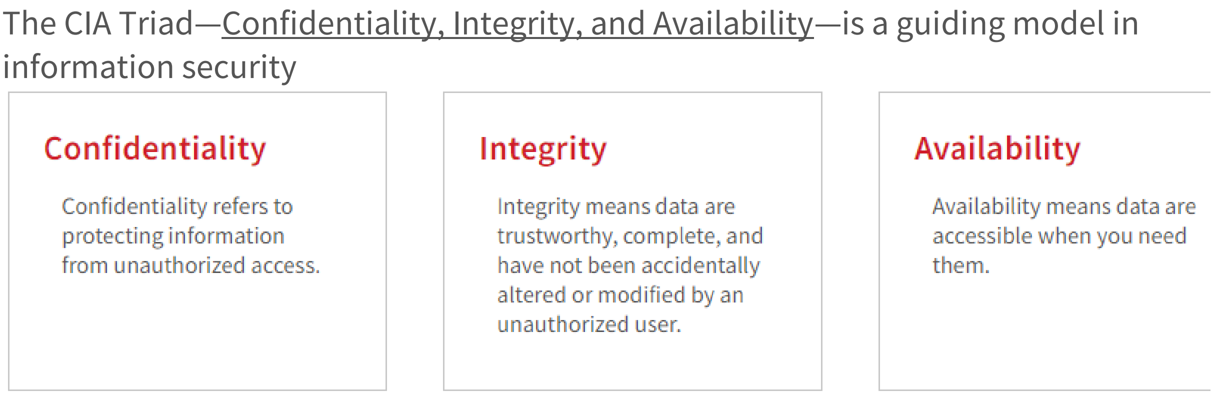
- As the number of online users has increased globally, governments throughout the world have enacted a large number of inconsistent privacy and security laws. This highly complex global legal framework is creating regulatory problems for companies. Approximately 50% countries have some form of data protection laws. Many of these laws conflict with those of other countries, or they require specific security measures. Other countries have no privacy laws at all.
- The absence of consistent or uniform standards for privacy and security obstructs the flow of information among countries (***transborder data flows*****).** The European Union, for one, has taken steps to overcome this problem. In 1998, the European Community Commission (ECC) issued guidelines to all of its member countries regarding the rights of individuals to access information about themselves.
- The transfer of data into and out of a nation without the knowledge of either the authorities or the individuals involved raises a number of privacy issues. Governments must make an effort to develop laws and standards to cope with rapidly changing information technologies to solve some of these privacy issues.
- Whose (which country's) laws have jurisdiction when records are stored in a different country for reprocessing or retransmission purposes?

1. Define ethics, list and describe the three fundamental tenets of ethics, and describe the four categories of ethical issues related to information technology.

2. 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.

Information Security

- **Security** can be defined as the degree of protection against criminal activity, danger, damage, and/or loss. Following this broad definition, **information security** refers to all of the processes and policies designed to protect an organization's information and information systems (IS) from unauthorized access, use, disclosure, disruption, modification, or destruction.
- A **threat** to an information resource is any danger to which a system may be exposed. The **exposure** of an information resource is the harm, loss, or damage that can result if a threat compromises that resource. An information resource's **vulnerability** is the possibility that the system will be harmed by a threat.



The CIA Triad—Confidentiality, Integrity, and Availability—is a guiding model in information security

Confidentiality

Confidentiality refers to protecting information from unauthorized access.

Integrity

Integrity means data are trustworthy, complete, and have not been accidentally altered or modified by an unauthorized user.

Availability

Availability means data are accessible when you need them.

What are the key factors contributing to the increasing vulnerability of organizational information resources

The five key factors are contributing to the increasing vulnerability of organizational information resources, making it much more difficult to secure them: (Explain each point in detail)

- Today's interconnected, interdependent, wirelessly networked business environment

(A *trusted network*, in general, is any network within your organization. An *untrusted network*, in general, is)any network external to your organization.

- Smaller, faster, cheaper computers and storage devices
- Decreasing skills necessary to be a computer hacker

(The reason is that the Internet contains information and computer programs called ***scripts*** that users with few skills can download and use to attack any information system connected to the Internet.)

- International organized crime taking over cybercrime

Groups of well-organized criminal organizations have taken control of a global billion-dollar crime network. The network, powered by skilful hackers, targets known software security weaknesses

- Lack of management support

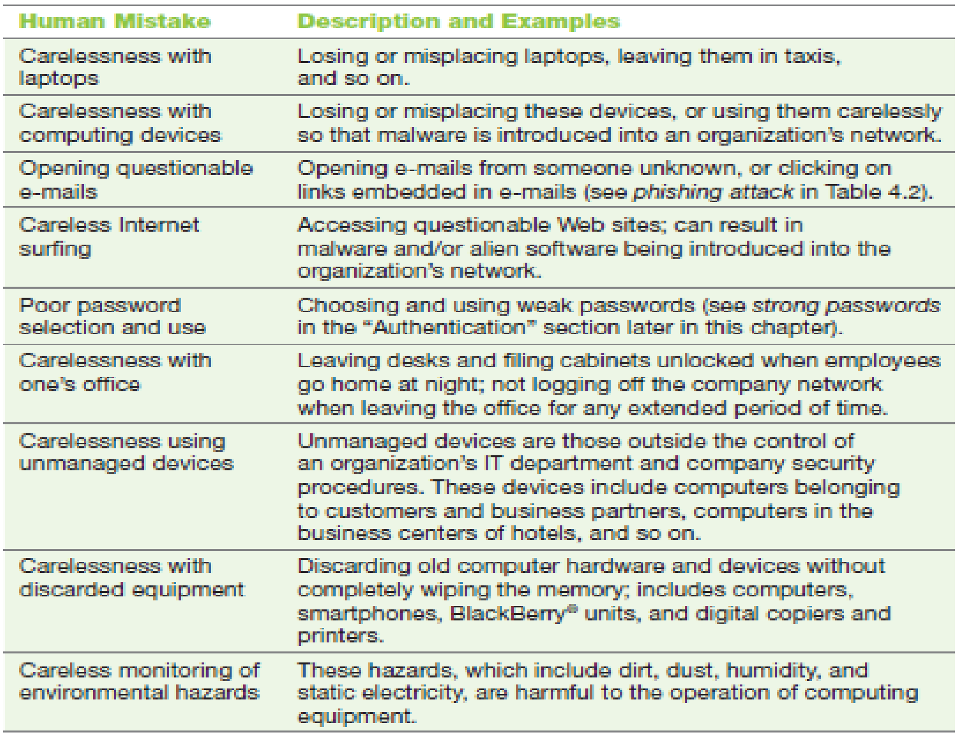
For the entire organization to take security policies and procedures seriously, senior managers must set the tone.

Explain the Threats to Information Systems

The two major categories of threats are **unintentional threats** and **deliberate threats**.

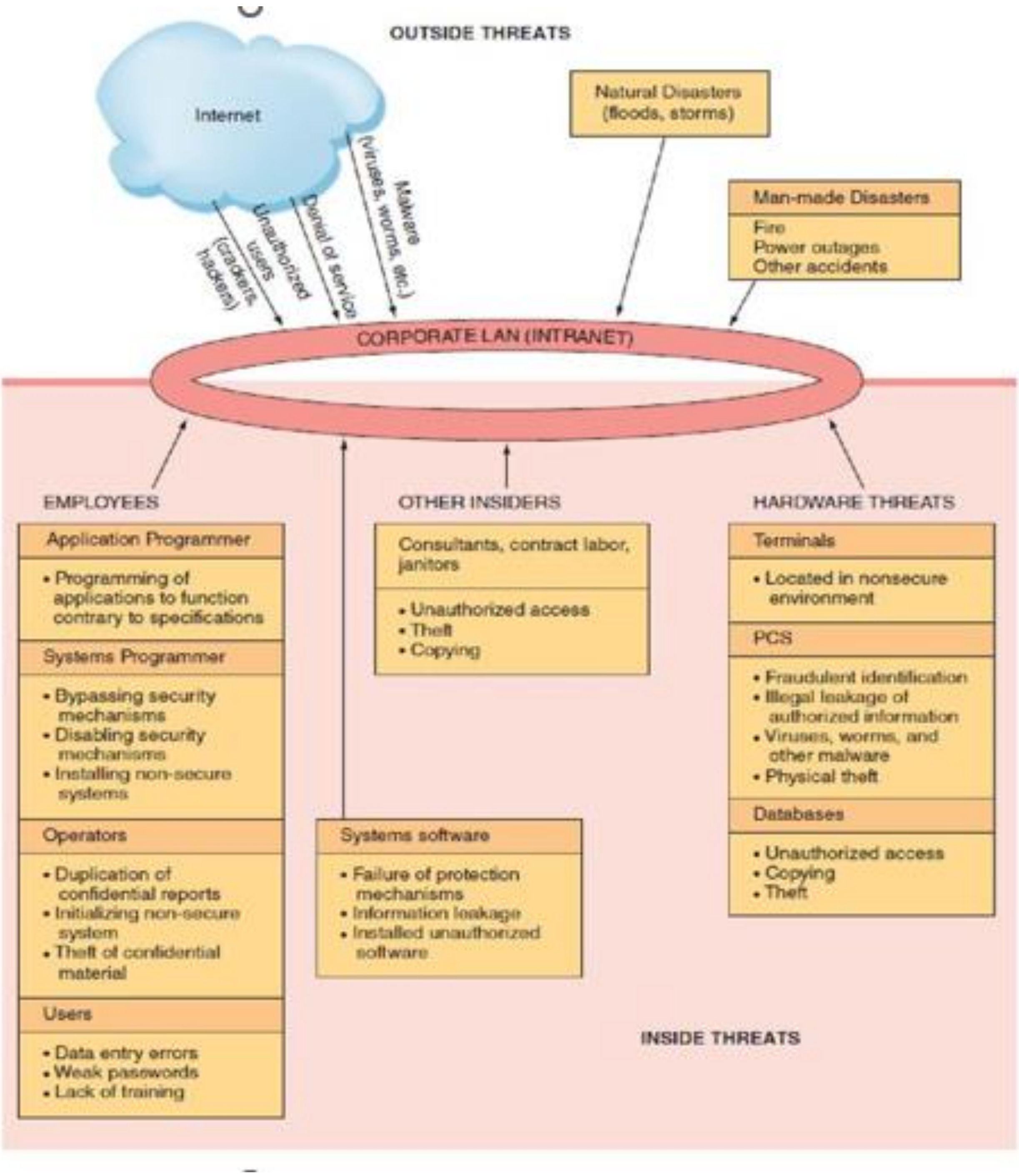
Unintentional threats to an information system: Through Human errors, Social Engineering etc.

Human Mistakes: (Examples)



Human Mistake	Description and Examples
Carelessness with laptops	Losing or misplacing laptops, leaving them in taxis, and so on.
Carelessness with computing devices	Losing or misplacing these devices, or using them carelessly so that malware is introduced into an organization's network.
Opening questionable e-mails	Opening e-mails from someone unknown, or clicking on links embedded in e-mails (see *phishing attack* in Table 4.2).
Careless Internet surfing	Accessing questionable Web sites; can result in malware and/or alien software being introduced into the organization's network.
Poor password selection and use	Choosing and using weak passwords (see *strong passwords* in the "Authentication" section later in this chapter).
Carelessness with one's office	Leaving desks and filing cabinets unlocked when employees go home at night; not logging off the company network when leaving the office for any extended period of time.
Carelessness using unmanaged devices	Unmanaged devices are those outside the control of an organization's IT department and company security procedures. These devices include computers belonging to customers and business partners, computers in the business centers of hotels, and so on.
Carelessness with discarded equipment	Discarding old computer hardware and devices without completely wiping the memory; includes computers, smartphones, BlackBerry® units, and digital copiers and printers.
Careless monitoring of environmental hazards	These hazards, which include dirt, dust, humidity, and static electricity, are harmful to the operation of computing equipment.

Figure: Security threats


OUTSIDE THREATS
Internet
Malware (viruses, worms, etc.)
Denial of service
Unauthorized users (crackers, hackers)
Natural Disasters (floods, storms)
Man-made Disasters
Fire
Power outages
Other accidents
CORPORATE LAN (INTRANET)
EMPLOYEES
Application Programmer
• Programming of applications to function contrary to specifications
Systems Programmer
• Bypassing security mechanisms
• Disabling security mechanisms
• Installing non-secure systems
Operators
• Duplication of confidential reports
• Initializing non-secure system
• Theft of confidential material
Users
• Data entry errors
• Weak passwords
• Lack of training
OTHER INSIDERS
Consultants, contract labor, janitors
• Unauthorized access
• Theft
• Copying
Systems software
• Failure of protection mechanisms
• Information leakage
• Installed unauthorized software
HARDWARE THREATS
Terminals
• Located in nonsecure environment
PCS
• Fraudulent identification
• Illegal leakage of authorized information
• Viruses, worms, and other malware
• Physical theft
Databases
• Unauthorized access
• Copying
• Theft
INSIDE THREATS

Provide examples of social engineering attacks

- **Social engineering** is an attack in which the perpetrator uses social skills to trick or manipulate legitimate employees into providing confidential company information such as passwords.
- The most common example of social engineering occurs when the attacker impersonates someone else on the telephone, such as a company manager or an information systems employee.
- Other common ploys include posing as an exterminator, an air-conditioning technician, or a fire marshal.

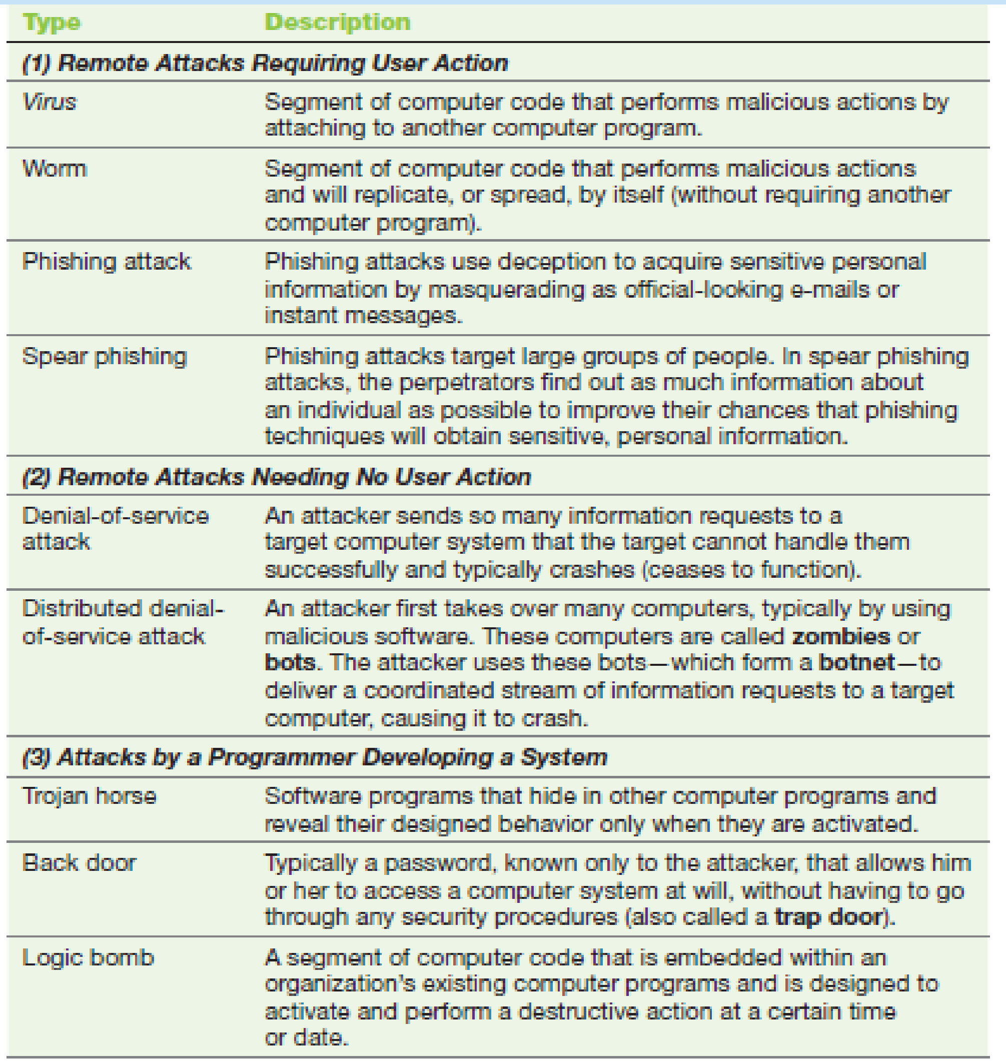
- Two other social engineering techniques are **tailgating and shoulder surfing**. ***Tailgating*** is a technique designed to allow the perpetrator to enter restricted areas that are controlled with locks or card entry. The perpetrator follows closely behind a legitimate employee and, when the employee gains entry, the attacker asks him or her to "hold the door." ***Shoulder surfing*** occurs when a perpetrator watches an employee's computer screen over the employee's shoulder. This technique is particularly successful in public areas such as in airports and on commuter trains and airplanes.

What are the Deliberate Threats to Information Systems (Explain points in detail)

There are many types of deliberate threats to information systems. We provide a list of 10 common types for your convenience.

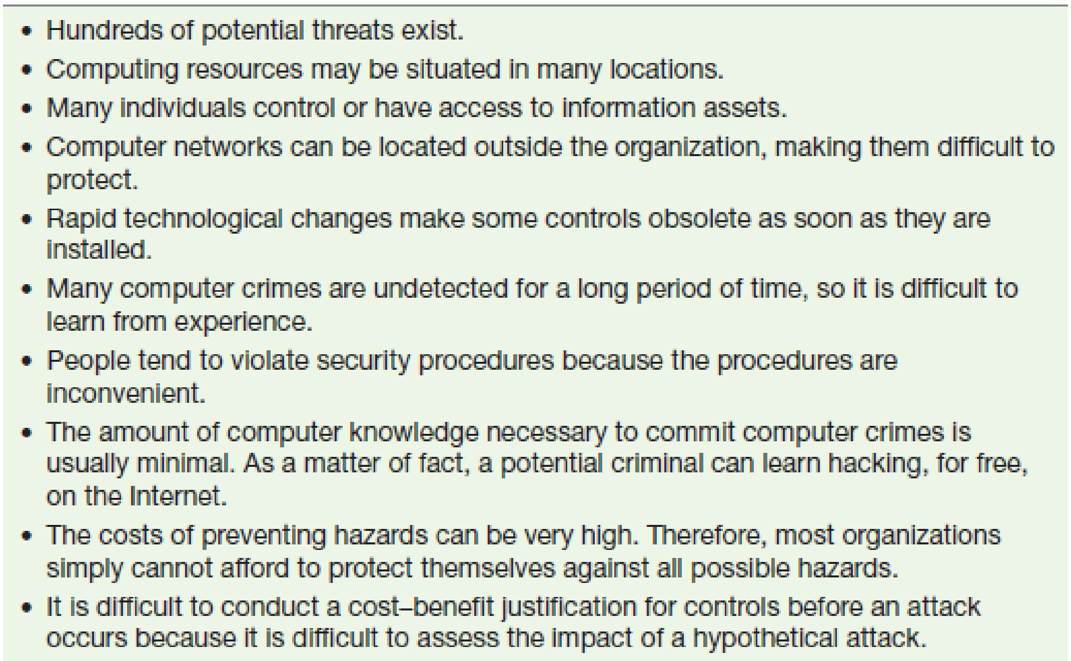
- Espionage or trespass
- Sabotage or vandalism
- Identity theft
- Software attacks
- Information extortion
- Theft of equipment or information
- Compromises to intellectual property
- Alien software
- Supervisory control and data acquisition (SCADA) attacks
- Cyberterrorism and cyberwarfare

Types of Software attacks



Type	Description
(1) Remote Attacks Requiring User Action	
Virus	Segment of computer code that performs malicious actions by attaching to another computer program.
Worm	Segment of computer code that performs malicious actions and will replicate, or spread, by itself (without requiring another computer program).
Phishing attack	Phishing attacks use deception to acquire sensitive personal information by masquerading as official-looking e-mails or instant messages.
Spear phishing	Phishing attacks target large groups of people. In spear phishing attacks, the perpetrators find out as much information about an individual as possible to improve their chances that phishing techniques will obtain sensitive, personal information.
(2) Remote Attacks Needing No User Action	
Denial-of-service attack	An attacker sends so many information requests to a target computer system that the target cannot handle them successfully and typically crashes (ceases to function).
Distributed denial-of-service attack	An attacker first takes over many computers, typically by using malicious software. These computers are called **zombies** or **bots**. The attacker uses these bots—which form a **botnet**—to deliver a coordinated stream of information requests to a target computer, causing it to crash.
(3) Attacks by a Programmer Developing a System	
Trojan horse	Software programs that hide in other computer programs and reveal their designed behavior only when they are activated.
Back door	Typically a password, known only to the attacker, that allows him or her to access a computer system at will, without having to go through any security procedures (also called a **trap door**).
Logic bomb	A segment of computer code that is embedded within an organization's existing computer programs and is designed to activate and perform a destructive action at a certain time or date.

Describe several reasons why it is difficult to protect information resources.



- Hundreds of potential threats exist.
- Computing resources may be situated in many locations.
- Many individuals control or have access to information assets.
- Computer networks can be located outside the organization, making them difficult to protect.
- Rapid technological changes make some controls obsolete as soon as they are installed.
- Many computer crimes are undetected for a long period of time, so it is difficult to learn from experience.
- People tend to violate security procedures because the procedures are inconvenient.
- The amount of computer knowledge necessary to commit computer crimes is usually minimal. As a matter of fact, a potential criminal can learn hacking, for free, on the Internet.
- The costs of preventing hazards can be very high. Therefore, most organizations simply cannot afford to protect themselves against all possible hazards.
- It is difficult to conduct a cost–benefit justification for controls before an attack occurs because it is difficult to assess the impact of a hypothetical attack.

Compare and contrast risk management, risk analysis and risk mitigation.

- Organizations spend a great deal of time and money protecting their information resources. Before doing so, they perform risk management.
- 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. Organizations perform **risk analysis** to ensure that their IS security programs are cost effective.
- Risk management consists of three processes: risk analysis, risk mitigation, and controls evaluation.
- **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.

What are the most important Information Security Controls in an organization

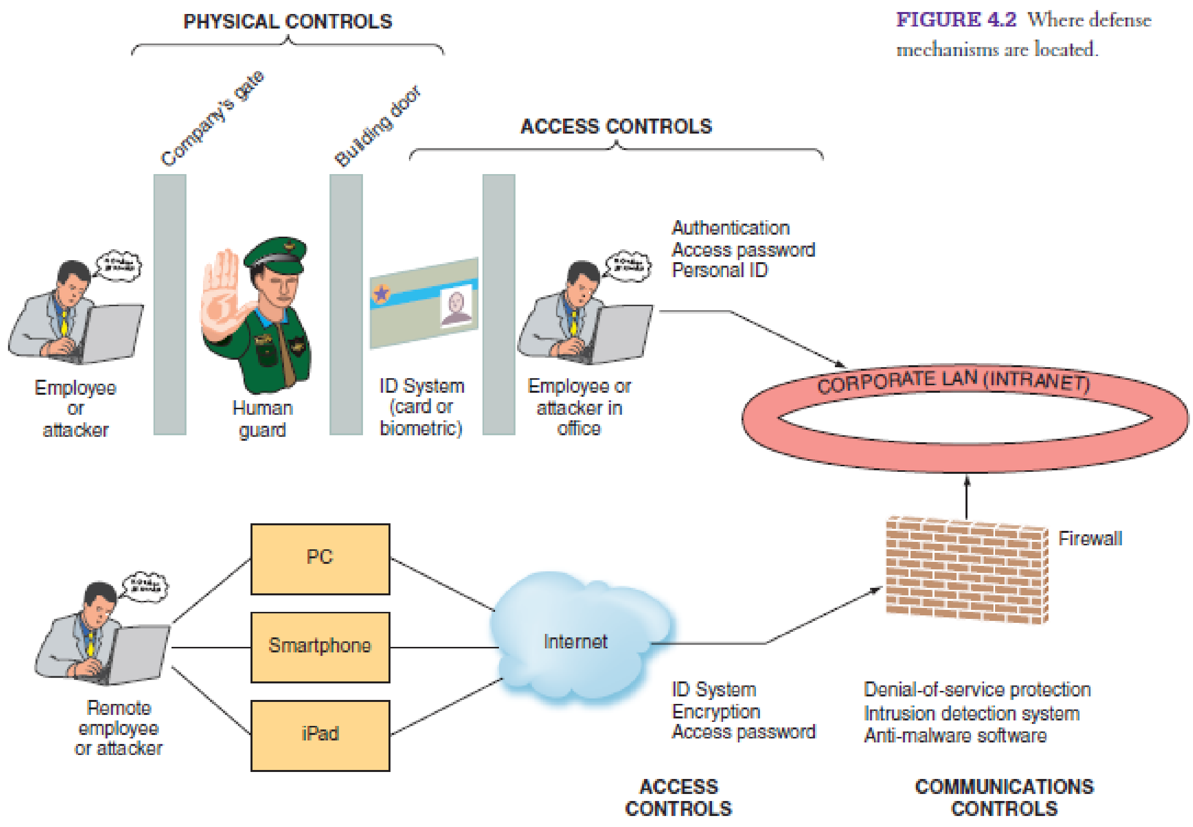


FIGURE 4.2 Where defense mechanisms are located.

(Explain each point in detail yourself)

✓ **Physical controls** prevent unauthorized individuals from gaining access to a company's facilities. Common physical controls include walls, doors, fencing, gates, locks, badges, guards, and alarm systems.

✓ **Access controls** restrict unauthorized individuals from using information resources. These controls involve two major functions: authentication and authorization. **Authentication (ex: biometrics)** confirms the identity of the person requiring access. After the person is authenticated (identified), the next step is authorization. **Authorization (ex: Passwords)** determines which actions, rights, or privileges the person has, based on his or her verified identity. Let's examine these functions more closely.

✓ All users should use *strong passwords*, which are difficult for hackers to discover. The basic guidelines for creating strong passwords are the following:

✓ • They should be difficult to guess. • They should be long rather than short.

- They should have uppercase letters, lowercase letters, numbers, and special characters.

✓ • They should not be recognizable words. • They should not be the name of anything or anyone familiar, such as family names or names of pets. • They should not be a recognizable string of numbers, such as a Social Security number or a birthday.

✓ A **privilege** is a collection of related computer system operations that a user is authorized to perform. Companies typically base authorization policies on the principle of **least privilege**, which posits that users be granted the privilege for an activity only if there is a justifiable need for them to perform that activity.

- ✓ **Communications controls** (also called **network controls**) secure the movement of data across networks. Communications controls consist of firewalls, anti-malware systems, whitelisting and blacklisting, encryption, virtual private networks (VPNs), transport layer security, and employee monitoring systems.
- ✓ **Transport layer security**, formerly called **secure socket layer**, is an encryption standard used for secure transactions such as credit card purchases and online banking. TLS encrypts and decrypts data between a Web server and a browser end to end.
- ✓ TLS is indicated by a URL that begins with "https" rather than "http," and it often displays a small padlock icon in the browser's status bar. Using a padlock icon to indicate a secure connection and placing this icon in a browser's status bar are artifacts of specific browsers.
- ✓ **Employee Monitoring Systems.** Many companies are taking a proactive approach to protecting their networks against what they view as one of their major security threats, namely, employee mistakes. These companies are implementing **employee monitoring systems**, which scrutinize their employees' computers, e-mail activities, and Internet surfing activities.
- ✓ **Business Continuity Planning:** **Business continuity** is the chain of events linking planning to protection and to recovery. The purpose of the business continuity plan is to provide guidance to people who keep the business operating after a disaster occurs. Employees use this plan to prepare for, react to, and recover from events that affect the security of information assets. The objective is to restore the business to normal operations as quickly as possible following an attack. The plan is intended to ensure that critical business functions continue.

1. Identify the three major types of controls that organizations can use to protect their information resources, and provide an example of each one.

(Physical control, Access control, Communication control) – Explained above + diagram

2. Define the three risk mitigation strategies, and provide an example of each one in the context of owning a home.

   The three risk mitigation strategies are the following:

   Risk acceptance, where the organization accepts the potential risk, continues operating with no controls, and absorbs any damages that occur. If you own a home, you may decide not to insure it. Thus, you are practicing risk acceptance. Clearly, this is a bad idea.

   Risk limitation, where the organization limits the risk by implementing controls that minimize the impact of threats. As a homeowner, you practice risk limitation by putting in an alarm system or cutting down weak trees near your house.

   Risk transference, where the organization transfers the risk by using other means to compensate for the loss, such as by purchasing insurance. The vast majority of homeowners practice risk transference by purchasing insurance on their houses and other possessions.