Etika, Privasi & Keamanan Informasi

Pertemuan ke-2

Universitas Bunda Mulia

Kompetensi Khusus

- Mahasiswa dapat menjelaskan isu etika dan privasi yang berhubungan dengan etika dalam penggunaan teknologi informasi dan ancaman serta tindakan penaggulangan pelanggaran teknologi informasi

Materi

1. Ethical Issues
2. Privacy
3. Introduction to Information Security
4. Unintentional Threats to Information System
5. Deliberate Threats to Information System
6. Information Security Controls

1. Ethical Issues

1.1 Ethics?

- 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 make ethical decisions.

1.2 Ethical Frameworks

- There are many sources for ethical standards. Here we consider four widely used standards:
  1. The utilitarian approach,
  2. The rights approach,
  3. The fairness approach, and
  4. The common good approach

1.2.1 The Utilitarian Approach (Lanj)

- 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.

1.2.1The Right Approach (Lanj)

- The right approach maintains that an ethical actions is the one that best protects and respects the moral rights of the affected parties.
- Moral right can include : The right to make one's own choices, to be told the truth, not be injured, and to enjoy a degree of privacy.
- An ethical organizational action would be one that protects and respects the moral rights of customers, employees, shareholders, business partners, and even competitors.

1.2.2 The Fairness Approach (Lanj)

- 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 firm.

1.2.2 The Fairness Approach (Lanj)

- 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.

1.2.3 The Common Good Approach

- 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.

1.2.4 The Common Good Approach

- These conditions can include a system of laws, effective police and fire departments, healthcare, a public educational system, and even public recreation areas.

1.3 General Framework for Ethics

If we combine these four standards we can develop a general frameworks. This frameworks consists five steps:

1. Recognize an ethical issues
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

1.4 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 examples:
    1. The Association of Computing Machinery (www.acm.org)
    2. The Organization of Computing Professionals

1.4 Ethics in the Corporate Environment (Lanj)

- Keep in mind that different codes of ethics are not always consistent with one another. Therefore, an individual might be expected to conform to multiple codes.
- For examples, a person who is a member of two large professional computing related organizations may be simultaneously required by one organization to comply with all applicable laws and by the organization to comply with all applicable laws and by the other organization to refuse to obey unjust laws.

1.4 Ethics in the Corporate Environment (Lanj)

- Fundamental tenets of ethics include:

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

1.5 Ethics and Information Technology

The diversity and ever-expanding use of IT applications have created a variety of ethical issues. These issues :

1. **Privacy** issues involve collecting, storing, and disseminating information about individuals.
2. **Accuracy** issues involve the authenticity, fidelity, and correctness of information that is collected and processed.
3. **Property** issues involved the ownership and value of information
4. **Accessibility** issues revolve around who should have access to information and whether they should pay a fee for this access

2. Privacy

2.1 What is Privacy?

- Privacy is the right to be left alone and to be free of unreasonable person intrusions.
- Information privacy is the right to determine when and to what extent, information about you can be gathered and/or communicated to other.
- Privacy right apply to individuals, groups, and institutions.

2.3 Electronic Surveillance

- According to the American Civil Liberties Union (ACLU), Tracking people activities with the aid of information technology has become a major privacy-related problem.
- 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.

2.3 Example of Electronic Surveillance

- Facial Recognition technology: this technology can now match faces even in regular snapshots and online images. For example Intel and Microsoft have introduce in store digital billboards that can recognize your face.
- These billboards can keep track of the product you are interested in based on your purchases or browsing behavior.

2.4Personal Information in Databases

Modern institutions store information about individuals in many databases. Perhaps the most visible locations of such records are 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.

2.5 Privacy Codes and Policies

- Privacy policies or privacy codes are an organization's guidelines for protecting the privacy of its customers, clients, and employees. In many corporations, senior management has begun to understand that when they collect vast amounts of personal information, they must protect it.

3. Introduction to Information Security

3.1 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

3.2 Threat vs Vulnerability

- 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.

3.3 Five Key Factor in Vulnerability

- Today, five key factors are contributing to the increasing vulnerability of organizational information resources, making it much more difficult to secure them:

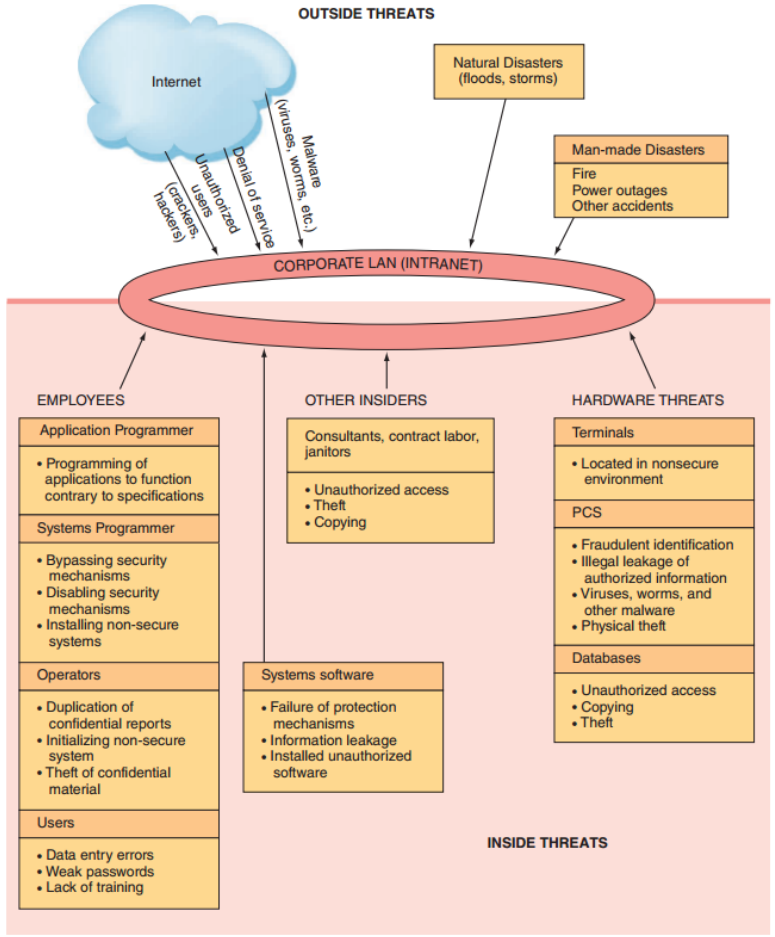
1. Interconnected, interdependent, wirelessly network business environment
2. Smaller, faster, cheaper computer and storage devices
3. Decreasing skill necessary to be a computer hacker
4. International organized crime taking over cybercrime
5. Lack of management support.

4. Unintentional Threats to Information Systems

4.1 Security Threats

- Information system are vulnerable to many potential hazards and threats. The two major categories of threats are unintentional threats and deliberate threats.

4.1 Security Threats (Lanj)



4.1 Human Error

- Organizational employees span the breadth and depth of the organization, from mail clerks to the CEO, and across all functional areas. There are two important points to be made about employees.

1. The Higher the level of employee
2. Human resources and information systems.

4.1.1 The Higher The Level Of Employee

- First, the higher the level of employee, the greater the threat he or she poses to information security. This is true because higher level employees typically have greater access to corporate data, and they enjoy greater privileges on organizational information systems.

4.1.2 Human Resources and Information Systems.

- Second, employees in two areas of the organization pose especially significant threats to information security: human resources and information systems. Human resources employees generally have access to sensitive personal information about all employees. Likewise, IS employees not only have access to sensitive organizational data but also often control the means to create, store, transmit, and modify those data

4.2 Social Engineering

- **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.

4.2 Social Engineering Techniques

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.”

4.2 Social Engineering Techniques

- 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.

5. Deliberate Threats to Information System

5.1 Threats to Information System

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

1. Espionage or Trespass
2. Information Extortion
3. Sabotage or Vandalism
4. Theft of Equipment or Information
5. Identity Theft
6. Compromises to Intellectual Proprty
7. Software Attacks
8. Alien Software
9. Supervisory Control & Data Acquisition (SCADA) Attacks
10. Cyberterrorism and Cyberwarface.

6. Information Security Controls

6.1 Information Security Controls

- To protect their information assets, organizations implement **controls**, or defense mechanisms (Countermeasures)
- Controls are designed to protect all of the components of an information system, including data, software, hardware, and network.
- Controls are intended to prevent accidental hazards, deter intentional acts, detect problems as early as possible, enhance damage recovery.

6.2 Types of Control

- In this section, we will learn types of controls such as:

1. Physical Control,
2. Access Control,

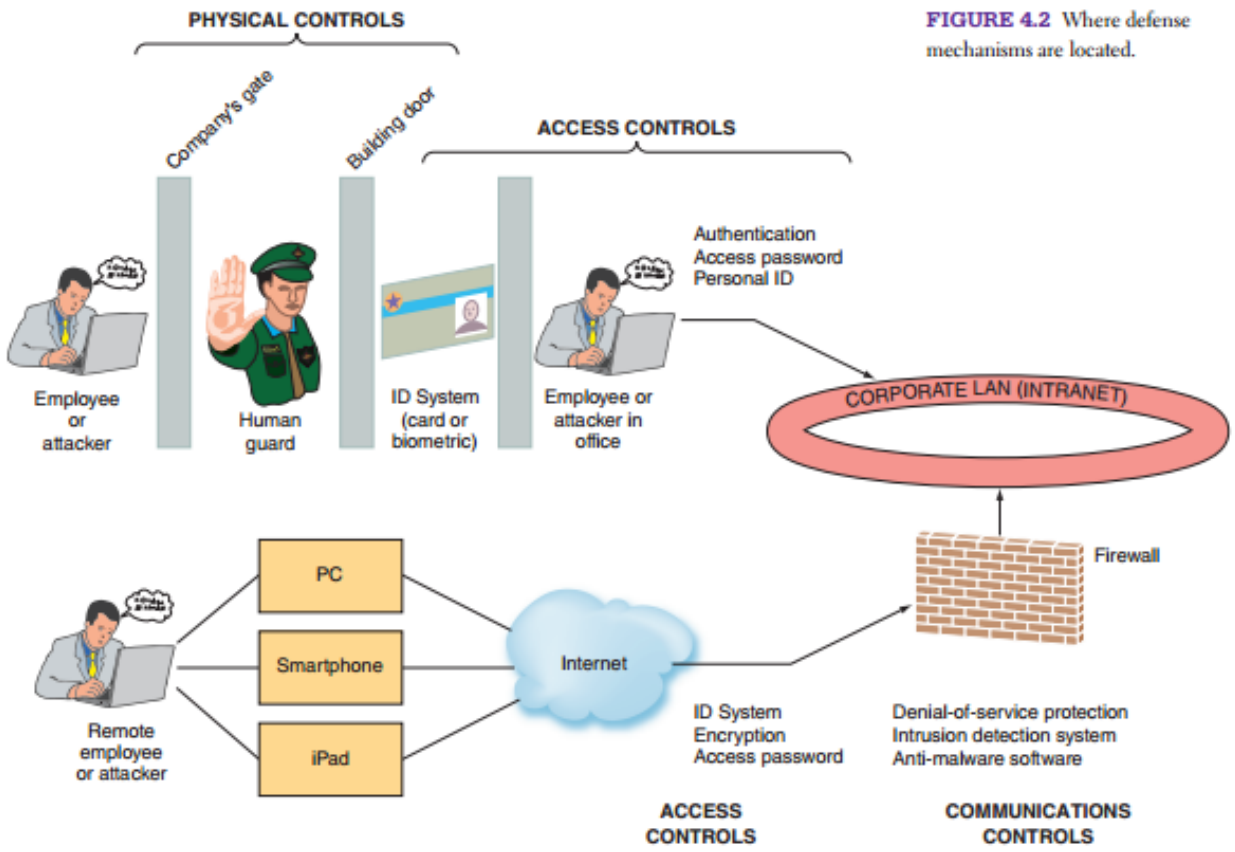


FIGURE 4.2 Where defense mechanisms are located.

6.1.1 Physical Controls

- **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. More sophisticated physical controls include pressure sensors, temperature sensors, and motion detectors. One shortcoming of physical controls is that can be inconvenient to employees.

6.1.1 Physical Controls (Lanj)

- Organizations also implement physical security measures that limit computer users to acceptable login times and locations. These controls also limit the number of unsuccessful login attempts, and they require all employees to log off their computers when they leave for the day. In addition, they set the employees' computers to automatically log off the user after a certain period of disuse

6.1.2 Access Controls

- **Access controls** restrict unauthorized individuals from using information resources. These controls involve two major functions: **authentication and authorization.**

6.1.2 Access Controls (Lanj)

- **Authentication** confirms the identity of the person requiring access. After the person is authenticated (identified), the next step is authorization.
- **Authorization** determines which actions, rights, or privileges the person has, based on his or her verified identity.

Summary:

- Ethics refers to the principles of right and wrong that individuals use to make choices that guide their behavior
- Fundamental tenets of ethics include responsibility, accountability, and liability.
- Major ethical issues related to IT are privacy, accuracy, property and access to information

Summary (Lanj)…

- 10 types of deliberate attacks such as : Espionage or trespass, information extortion, sabotage, theft of equipment and information, identity theft, software attacks, supervisory control and data acquisition.
- There are three risk mitigation strategies such as : Risk acceptance, Risk Limitation, Risk Transference.
- Three major types of control that organization to protect their information resources such as: Physical controls, access controls, communications controls.