Ethical Issues & Privacy

Ethics

- Ethics
  - A branch of philosophy that deals with what is considered to be right and wrong.
- A Code of Ethics
  - A code of ethics is a collection of principles intended as a guide for members of a company or organization.

Example: Facebook-Cambridge Analytica Scandal

Context: In 2018, it was revealed that Cambridge Analytica, a political consulting firm, had improperly accessed the personal data of millions of Facebook users without their consent. This data was used to create detailed voter profiles and influence the 2016 U.S. presidential election.

Ethical Terminology

- Responsibility
  - means that you accept the consequences of your decisions and actions.
- Accountability
  - means a determination of who is responsible for actions that were taken.
- Liability
  - a legal concept meaning that individuals have the right to recover the damages done to them by other individuals, organizations, or systems.

Target Data Breach (2013)

Context: In 2013, Target, one of the largest retail chains in the U.S., suffered a massive data breach during the holiday shopping season. Hackers gained access to the credit and debit card information of over 40 million customers, as well as personal information, including names, addresses, phone numbers, and email addresses, of an additional 70 million customers.

Ethical Issues

- The diversity and ever expanding use of IT applications have created a variety of ethical issues.
- These issues fall into four general categories:
  - 1. Privacy issues involve collecting, storing, and disseminating information about individuals.
  - 2. Accuracy issues involve the authenticity, fidelity, and accuracy of information that is collected and processed.
  - 3. Property issues involve the ownership and value of information.
  - 4. Accessibility issues revolve around who should have access to information and whether they should have to pay for this access.

Ethical Issues &Privacy

- The use of information systems and technology impacts individuals, groups, and societies. Technology must be used ethically and designed to avoid injuring humans.

Autonomous Vehicles and AI Decision-Making

Context: Autonomous vehicles (self-driving cars) rely on complex algorithms and artificial intelligence (AI) to make decisions on the road, such as how to navigate traffic, avoid obstacles, and respond to unexpected situations. These decisions can directly impact human safety.

Ethical Issues

- Policies and procedures must be established to avoid computer waste and mistakes.
- Although often unintentional, computer waste and mistakes can be costly. Organizational policies & procedures can help avoid losses.
- Intentional computer crime is rapidly increasing and requires the attention of management and security specialists.

Computer Waste

- Discard technology
- Unused systems
- Personal use of corporate time and technology

Computer Waste

- Computer waste is widespread in the public and private sectors, and is usually caused by the improper management of information technology.
- Some companies discard usable hardware and software that could be used elsewhere in the company, or sold or donated.
- Another example of computer waste occurs when significant resources are invested in the development of an information system, and then, it is never used to it fullest extent.
- This happens for many reasons, but poor design and inadequate training are major causes. Employees playing computer games or surfing the Web at their desks during working time is also a source of waste, as are junk e-mail and junk faxes.

Preventing Computer Waste and Mistakes

- Establish Policies and Procedures
- Implement Policies and Procedures
- Monitor Policies and Procedures
- Review Policies and Procedures
- Procedures relating to the acquisition and use of computers can avoid both waste and mistakes.
- For example, procedures could ensure that computers no longer needed in one part of the company would be used in another part, rather than discarded.

Preventing Computer Waste and Mistakes

- Employees and groups are less likely to make mistakes using applications and technology if they have been properly trained in their use.
- Many organizations require that systems or applications meeting certain criteria must be approved by a committee or the IS department before they are acquired or implemented, to ensure they are compatible with existing systems, databases, and technology, and are cost-effective.
- Many organizations have established procedures to ensure that all systems, including those developed by end users, have adequate documentation.

Why to secure information

- Recognize that organizations have a business need for information security
- Understand that a successful information security program is the responsibility of both an organization's general management and IT management
- Identify the threats posed to information security and the more common attacks associated with those threats, and differentiate threats to the information within systems from attacks against the information within systems

Information Security

- Primary mission of information security is to ensure systems and contents stay the same
- If no threats, could focus on improving systems, resulting in vast improvements in ease of use and usefulness
- Attacks on information systems are a daily occurrence

What Business Needs

- Information security performs four important functions for an organization
  - Protects ability to function
  - Enables safe operation of applications implemented on its IT systems
  - Protects data the organization collects and uses
  - Safeguards technology assets in use
  - Organization should address information security in terms of business impact and cost

Threats

- Threat: an object, person, or other entity that represents a constant danger to an asset
- Management must be informed of the different threats facing the organization
- By examining each threat category, management effectively protects information through policy, education, training, and technology controls

Categories of Threats

Categories of threat	Examples
1. Acts of human error or failure	Accidents, employee mistakes
2. Compromises to intellectual property	Piracy, copyright infringement
3. Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
4. Deliberate acts of information extortion	Blackmail of information disclosure
5. Deliberate acts of sabotage or vandalism	Destruction of systems or information
6. Deliberate acts of theft	Illegal confiscation of equipment or information
7. Deliberate software attacks	Viruses, worms, macros, denial-of-service
8. Forces of nature	Fire, flood, earthquake, lightning
9. Deviations in quality of service from service providers	Power and WAN service issues
10. Technical hardware failures or errors	Equipment failure
11. Technical software failures or errors	Bugs, code problems, unknown loopholes
12. Technological obsolescence	Antiquated or outdated technologies

Information System Ethics

Computer Literacy

- Knowing how to use a computer

Digital Divide

- That gap between those with computer access and those who don't have it

Computer Ethics

- Standards of conduct as they pertain to the use of information systems

Information System Ethics

Privacy

- Protecting one's personal information

Identity theft

- Stealing of another's social security number, credit card number, or other personal information

Information System Ethics

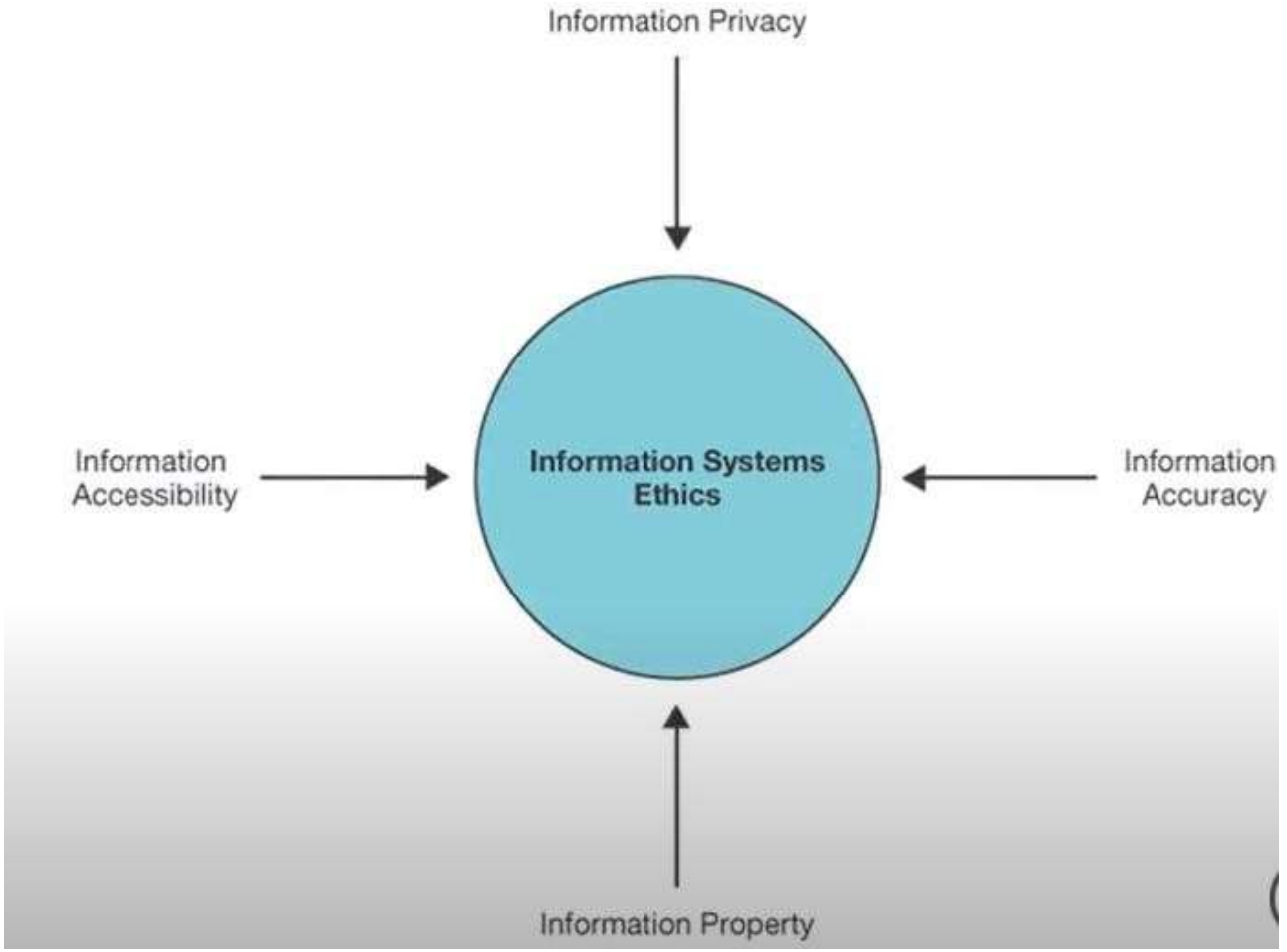
Information accuracy

- Deals with authentication and fidelity of information

Information property

- Deals with who owns information about individuals and how information can be sold and exchanged

Information System Ethics



Information System Ethics

Information accessibility

- Deals with what information a person has the right to obtain about others and how the information can be used

Issues in information accessibility

- Carnivore: software application designed to be connected to Internet Service Providers' computers and eavesdrops on all communications.
- Electronic Communications Privacy Act (ECPA): it offered stronger support for voice mail than it did for e-mail. No other laws at federal or state levels protect e-mail privacy
- Monitoring e-mail

Information System Ethics

The need for a code of ethical conduct

- Business ethics
- Plagiarism
- Cybersquatting: registering a domain name and then trying to sell the name for big bucks to a person, company. Domain names are a scarce resource – one of the few scarce resources in cyberspace

Computer Crime

Definition: the act of using a computer to commit an illegal act

- Authorized and unauthorized computer access
- Examples
  - Stealing time on company computers
  - Breaking into government Web sites
  - Stealing credit card information

Computer Crime

Federal and State Laws

- Stealing or compromising data
- Gaining unauthorized computer access
- Violating data belonging to banks
- Intercepting communications
- Threatening to damage computer systems
- Disseminating viruses

Hacking and Cracking

- Hacker – one who gains unauthorized computer access, but without doing damage
- Cracker – one who breaks into computer systems for the purpose of doing damage

Information System Ethics

Computer viruses and destructive code

- Virus – a destructive program that disrupts the normal functioning of computer systems
- Types:
  - Worm: usually does not destroy files; copies itself
  - Trojan horses: Activates without being detected; does not copy itself
  - Logic or time bombs: A type of Trojan horse that stays dormant for a period of time before activating

Computer Security

Computer Security – precautions taken to keep computers and the information they contain safe from unauthorized access

Recommended Safeguards

- Implement a security plan to prevent break-ins
- Have a plan if break-ins do occur
- Make backups!
- Only allow access to key employees
- Change passwords frequently
- Keep stored information secure
- Use antivirus software
- Use biometrics for access to computing resources
- Hire trustworthy employees

Computer Security

Encryption – the process of encoding messages before they enter the network or airwaves, then decoding them at the receiving end of the transfer

What is Information Security?

Information security is defined as the practice of protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

Security as a Non-Functional Requirement:

•Security is considered a non-functional requirement. This means that it is not about what the system does (its functionality) but about how the system operates. The assumption here is that the system must be correctly implemented according to its functional specifications to ensure security.

System Operation According to Intention:

•Security ensures that the system operates according to its intended purpose, preventing unauthorized actions that could compromise its functionality.

Security as a Process, Not a Product:

Security is not something that can be fully achieved by simply buying a product. Instead, it is a continuous process involving:

- Specification of the System
- Design and Implementation
- Installation and Operation:
- Human Factors

Information is an Asset

- Security is against the confidentiality of the data, integrity of data/information availability of the data

What is information

- Information is the lifeblood of modern civilization.
  - In the form of data it is the raw material from which understanding and, ultimately, controls are fashioned.
  - Compiled, analyzed, considered and reported, it is an asset and a currency of exchange.
  - As ideas and concepts it is the intellectual capital that shores up our economic system and our way of life.
- Information can be stored, moved easily and cheaply from place to place, and replicated ad infinitum.

What is Information

- It is a form of knowledge that we acquire through education, communication, practical experience, research, analysis.
- It consists of data, facts, and conclusions.
- To the engineer it is any data that can be expressed as a sequence of ones and zeros.

Five key factors increasing vulnarability

1. Today's interconnected, interdependent, wirelessly networked business environment
2. Smaller, faster, cheaper computers and storage devices
3. Decreasing skills necessary to be a computer hacker
4. International organized crime taking over cybercrime
5. Lack of management support

Today’s interconnected, interdependent, wirelessly networked business environment:

Example:

Modern businesses often rely on cloud services, internet-connected devices, and wireless networks to operate efficiently.

For example, a retail company might use cloud-based software for inventory management, point-of-sale systems, and customer relationship management (CRM).

This interconnectedness means that if one part of the system is compromised, it could affect the entire operation.

A hacker gaining access to the company's CRM system through a vulnerable wireless network could steal sensitive customer information.

Smaller, faster, cheaper computers and storage devices:

Example:
The proliferation of affordable and powerful devices, such as USB drives, smartphones, and microcomputers like the Raspberry Pi, has made it easier to store and transfer large amounts of data quickly.

While this is beneficial for legitimate uses, it also makes it easier for cybercriminals to steal and transport sensitive information.

For instance, an employee might accidentally lose a USB drive containing unencrypted customer data, leading to a data breach.

Decreasing skills necessary to be a computer hacker:

Example: Hacking has become more accessible due to the availability of ready-made tools and scripts that require little technical expertise.

For instance, "script kiddies" can use software like automated SQL injection tools or pre-built malware kits available on the dark web to launch cyberattacks without needing in-depth knowledge of coding or networks.

This increases the number of potential attackers.

International organized crime taking over cybercrime:

Example:
Organized crime groups have recognized the profitability of cybercrime and have expanded into this area.

For instance, ransomware attacks, where hackers encrypt a company's data and demand payment to release it, are often orchestrated by well-organized international groups.

These groups operate across borders, making it difficult for law enforcement to track and stop them.

Lack of management support:

Example: If company leadership does not prioritize cybersecurity, it can lead to inadequate security measures, such as not investing in proper training for employees or not implementing robust security protocols.

For example, if a company's management dismisses the importance of regular software updates, this can leave systems vulnerable to known exploits, which hackers can easily take advantage of.

Two main Types of threats

- Unintentional
- Intentional

Unintentional

- Carelessness with computing device
- Opening questionable emails
- Carless Internet surfing
- Poor password strength
- Carelessness in the office

Carelessness with computing devices: This refers to not properly securing devices like laptops, smartphones, or tablets. For example, leaving a laptop unattended in a public place where it could be stolen.

Opening questionable emails: This involves opening or interacting with emails from unknown or suspicious sources, which may contain phishing links or malware. For instance, receiving an email claiming you've won a prize and clicking on the link without verifying its authenticity.

Careless Internet surfing: This refers to visiting untrusted websites, which might expose your computer to viruses or malicious software. For example, downloading software from a sketchy website without checking if it’s safe.

Poor password strength: Using weak passwords that are easy to guess or using the same password across multiple sites. An example is using "password123" as a password, which can be easily cracked by hackers.

Carelessness in the office: This includes behaviors like leaving sensitive documents on your desk or not locking your computer when you step away. For instance, walking away from your desk without locking your screen, leaving your computer open to unauthorized access.

Intentional

- Espionage, trespass, extortion
- Theft of equipment or information
- Identity theft
- Software attacks

Espionage, trespass, extortion:

Espionage: This involves the practice of spying or using spies to obtain confidential information. For example, a competitor might hire someone to infiltrate a company and steal trade secrets.

Trespass: Unauthorized entry into someone's property, including digital spaces like networks or computers. For instance, a hacker gaining access to a company's internal network without permission.

Extortion: Forcing someone to give up something valuable, usually money, by threatening harm. An example is a cybercriminal who demands ransom from a company, threatening to release stolen data if they don't pay.

Theft of equipment or information:
This refers to stealing physical devices like laptops, smartphones, or hard drives, or stealing data and confidential information. For example, a thief might steal a laptop from an office, gaining access to sensitive company data stored on the device.

•**Identity theft**:

•This occurs when someone unlawfully obtains and uses another person's personal information, typically for financial gain. For example, a criminal might steal your Social Security number to open credit accounts in your name, leading to financial loss and damaged credit.

•**Software attacks**:

•These are attacks that involve the use of malicious software (malware) to damage, disrupt, or gain unauthorized access to computer systems. For example, a ransomware attack where malware encrypts a user's files and demands payment for the decryption key.

Information Can be

- Created
- Modified
- Stored
- Destroyed
- Processed
- **Used – (For proper & improper purposes)**
- Transmitted
- Corrupted
- Lost
- Stolen

Information can be

- Printed or written on paper
- Stored electronically
- Transmitted by post or using electronics means
- Shown on corporate videos
- Displayed / published on web
- Verbal – spoken in conversations

Critical Characteristics of Information

The value of information comes from the characteristics it possesses.

- Availability
- Accuracy
- Authenticity
- Confidentiality
- Integrity
- Utility

Controlling Information System

- There are numerous threats to Information Systems
  - Hardware failures
  - Software failures
  - Upgrade issues
  - Disasters
  - Malicious intent

Controlling Information System

- Implemented through
  - Policies
  - Procedures
  - Standards
- Control must be thought about through all stages of Information Systems analysis, construction, deployment operations and maintenance

Controls

- General controls
  - Controls for design, security and use of Information Systems throughout the organisation
- Application controls
  - Specific controls for each application
  - User functionality specific

General Controls

- Implementation controls
  - Audit system development
  - Ensure properly managed and controlled
  - Ensure user involvement
  - Ensure procedures and standards are in use
- Software controls
  - Authorised access to systems

General Controls

- Hardware controls
  - Physically secure hardware
  - Monitor and fix malfunction
  - Environmental systems and protection
  - Backup of disk-based data

General Controls

- Computer operations controls
  - Day-to-day operations of Information Systems
  - Procedures
  - System set-up
  - Job processing
  - Backup and recovery procedures

General Controls

- Data security controls
  - Prevent unauthorised access, change or destruction
  - When data is in use or being stored
  - Physical access to terminals
  - Password protection
  - Data level access controls

General Controls

- Administrative controls
  - Ensure organisational policies, procedures and standards and enforced
  - Segregation of functions to reduce errors and fraud
  - Supervision of personal to ensure policies and procedures are being adhered

Application Controls

- Input controls
  - Data is accurate and consistent on entry
  - Direct keying of data, double entry or automated input
  - Data conversion, editing and error handling
  - Field validation on entry
  - Input authorisation and auditing
  - Checks on totals to catch errors

Application Controls

- Processing controls
  - Data is accurate and complete on processing
  - Checks on totals to catch errors
  - Compare to master records to catch errors
  - Field validation on update

Application Controls

- Output controls
  - Data is accurate, complete and properly distributed on output
  - Checks on totals to catch errors
  - Review processing logs
  - Track recipients of data

Protecting Your Privacy

- Use strong passwords
- Adjust privacy settings on your computer
- Surf the Web anonymously
- E-mail anonymously
- Erase your Google search history

Protecting Information Systems

- Information Systems, especially TPS, require high degrees of availability
- Technology is available to ensure systems are available and contain accurate information

Information Security

- The application of technology and processes to protect data from accidental or intentional misuse persons known or unknown inside or outside of an organization.
- By no means strictly a technical aspect, its technical aspects (firewalls, encryption, access controls, etc.) are important, but so are processes applied to ever varying situations.
- An increasingly high-profile problem as hackers (or crackers) take advantage of vulnerabilities against parts of an organization's network either Internet accessible or internal.