Business Education

Information Technology

DATA INTEGRITY AND SECURITY

Definition: Data integrity refers to the validity of data.
Data is said to have integrity if it is accurate and complete when it enters a system and does not become inaccurate after further processing. Data integrity can be comprised in a number of ways:

- Inaccurate data entry
- Viruses
- Hardware malfunctions
- Accidental or malicious deletion or changing of data
- Natural disasters such as fires, floods and earthquakes

Data security is a method used to ensure that data maintains integrity. This usually involves: physical safeguards and software safeguards.

Physical Safeguards (Restrictions)
This deals with the protection of hardware and software from accidental or malicious damage or destruction. For instance:

1. Use of a monitoring system using video cameras
2. Security guards
3. Storing data in a fire/water proof safe
4. Storing data in another building or in another location
5. Distributing sensitive work to a number of employees rather than just one.

Software Safeguards (Restrictions)
This prevents unauthorised access to computer files. For instance:
1. **Using passwords**:
a. To access the system. A user would be required to enter a password or PIN (Personal Identification Number) to gain access to the system.
b. For individual files within a system

2. **Data Encryption**: encoding (scrambling) data during storage or transmission so that it cannot be understood by someone who does not have the encryption key (software to convert it back to its original form).

3. **Installing a Firewall**. This is a program, hardware device or a combination of both that filters the information coming in through the Internet connection to your computer system or network. It prevents unauthorised users from gaining access. Some firewalls protect systems from viruses and spam (electronic junk mail). Two popular firewall software packages are

BlackIce Defender and Zone Alarm.

MISUSE OF INFORMATION

Organisations gather information from a wide variety of sources including employees, suppliers, customers and competitors. When information is voluntarily provided to an organisation, it is usually for a specific purpose, e.g. for hospitals, clinics, insurance agencies etc.

Measures should therefore be in place to ensure that information is not misused. However, security breaches are common. Also, the use of information for purposes other than that which it was originally intended for is also common. Some countries have legislation that seeks to protect individuals from the potential misuse of information, such as:

1. Information should be used only for the purpose for which it was provided

2. The individual has the right to examine the contents of any personal record representing the individual.

3. The information must be accurate.

4. Security measures must be put into place to protect information.

5. The privacy of the individual must be protected.

COMPUTER CRIMES

Computers have given employees new tools that makes their jobs easier and allowed them to do things that was not possible before. Unfortunately, this is also true for criminals.

Definition: A **computer crime** is any illegal action where the data on a computer is accessed without permission.

This access doesn't have to result in loss of data or even data modifications. The worst computer crime occurs when there are no indications that data was accessed. Computer crime is often committed by hackers and crackers, but increasingly organized crime groups have realized the relative ease of stealing data with relative low-level of risk.

Definition: A **hacker** is a person who breaks into computers and computer networks, either for profit or just to prove that they can.

Definition: A **cracker** is someone who breaks into someone else's computer system, often on a network; bypasses passwords or licenses in computer programs.

Computer crimes include the following:

1. **Unauthorised Access** - This usually involves 'hacking' or 'cracking'. Some hackers see their activities as a form of game-playing, where they try to match their skills against other hackers, others have more destructive intentions such as breaking into an organisation's computer system to commit acts like **'electronic vandalism'** (e.g. deleting files, corrupting software, and changing critical data).

2. **Electronic Eavesdropping** - This is the use of electronic devices to monitor electronic communications between 2 or more groups without permission from either group. It includes computer data communications, voice, fax, landlines and mobile phones (e.g. the wire-tapping fiasco). This results in invasion of the privacy of individuals and organisations.

3. **Industrial Espionage** - Occurs when an organisation tries to gain an advantage on their competitors by illegally gaining access to information about marketing strategies, research & development, expansion plans etc. In the past, this was done by break-ins, illegal photograhing of documents and insiders passing out information. Now it can be acheived by hacking into the organisation's databases and viewing the informaiton.

4. **Surveillance** - Computer surveillance involves the use of technology to gather information from the user and from the computer without the user's knowledge. This can result in : i. loss of privacy of the user, ii. lack of security and iii. misuse of information (usually for monetary gain). There are several techniques for surveillance:

a. **Monitoring with utility software** - all data that passes in and out of a network or an individual's computer can be monitored. This is also known as **'packet sniffing'**, where a packet is the message being checked. Messages can be monitored by utility software (such as Packet Analyzer)or by using a computer on a network which can observe all packets passing through the network.

b. **Hardware devices** - by use of devices called **'bugs'** or a **'keystroke logger'** which is implanted into a keyboard.

c. **Monitoring from a distance** - done by the use of commercially available equipment which can receive and process the radiation emitted by the monitor. Data being displayed on the screen at the moment can then be observed without the knowledge of the user.

5. **Copyright and Piracy**

Definition: Copyright is the name given to the protection law of the rights of the person(s) responsible for creating items such as text, a piece of music, a painting or a computer program.

Consider the application Microsoft Word, which was written and improved by hundreds of programmers. If someone else were to copy the program code or steal it, it would be both unfair and illegal. A copyright law (enforced by the **Intellectual Properties Affairs** office in a country) would make it a criminal offence to be caught copying or stealing software.

Definition: Software piracy is the theft of computer programs and the unauthorised distribution and use of these programs.

The main types of piracy include:

a. Copying software (and its packaging) to look like the original product

b. Copying and selling recordable CD-ROMs that contained pirated software

c. Downloading software from the Internet

d. Use of software on two or more computers on a network if the license does not allow it.

6. **Propaganda** - Propaganda is the manipulation of public opinion. It is generally carried out through media that is capable of reaching a large amount of people and effectively persuading them for or against a cause. Computer systems can distribute information in such a manner that can be either beneficial or harmful material. An example of propaganda is using the Internet to sway public support of one party group or another in an attempt to discredit the opposing groups during an election (an electronic form of an election campaigns).

Software Piracy

What is software piracy?

Software piracy is a copying of a programs without the consent of the owner. It can also mean the unauthorized copying, use or selling of software that is copyrighted. It has become huge problem for software manufacturers because it causes loss of revenue and jobs

Types of software piracy

- **Counterfeiting**
- **Internet piracy**
- **End user piracy**
- **Client server over use**
- **Hard disk loading**

Measures to reduce software piracy.

- Use of registration keys that are only available with purchase of the software.
- Severe penalties such as heavy fines and/or imprisonment for anyone found selling or knowingly using pirated software
- Tamper proofing prevents people from pirating the software through the manipulation of the program's code. If the software is tampered with the program can shut down the software and then the software will stop work.
- License agreement this indicate the number of computers that can used a software package.

Unauthorized collection of information

A lot of information that is collected is done without the permission of the people involved. Three unauthorized collection of information are electronic eavesdropping, industrial espionage and surveillance.

- Industrial espionage- this is when secret information is obtained by spying on competitors or opponents illegally. Industrial espionage is conducted by companies for commercial purposes rather than governments for national security purposes. Industrial espionage may also be referred to as "corporate spying or espionage," or "economic espionage.

- Electronic eavesdropping-. As the term eavesdropping means to listen secretly to a person's conversation. Electronic eavesdropping is tapping into a communication channel to retrieve personal information without the participant consent. . Data may be encrypted before it is stolen to prevent eavesdropping on that data. Hackers can use electronic eavesdropping to collect information such as your credit card number, password or bank account details.

- Surveillance – the computer related activities of the internet are often kept under surveillance. The information gathered through this surveillance may be used to develop a profile of several people. An Internet Service Providers (ISP) can track all the websites you connect to, which means they know everything about your browsing habits. They can also see everything you send over the internet that isn't encrypted.

Unauthorized distribution of information

It is quite common for information that has been collected on an individual or company to be distributed without permission. For example sometimes we receive junk emails from companies that are advertising their products. The internet has made the unauthorized distribution of information very easy since many databases can be accessed about anyone with an internet connection. For example, information such as your name, address and date of birth can be seen on different social media platform such as Facebook.

Information Misuse

Information can be misused by the following ways:

- By collecting information about a person without their permission
- By a vengeful employees or employer who want to spread propaganda on innocent persons
- By storing incorrect information on an innocent person that might be available to the public
- When unauthorized persons are able to view and change your information
- By using information for purposes other than those for which it was intended for

Ways to reduce misuse of information

- Enforcing data protection laws
- Utilizing security systems
- Keep information accurate and updated
- Having severe penalties for persons who divulge private information.

Data Protection Law

Everyone has a fundamental right when it comes on to his/her personal information. In recognition of these rights such as information privacy, countries have developed a data protection law. The data protection law generally states that personal data must:

- Be obtained and process fairly and lawfully
- Be help for specified purposes
- Not be used for any incompatible with its original purpose
- Be relevant and adequate
- Be accurate and up to date
- Not to be kept longer than necessary
- Be made available to the individual concern and provision made for correction
- Be kept secured.

ACTIVITIES

Data Integrity and Security Part 1

Instruction: State whether the information is True or False

1. A firewall is a form of computer software protection.
2. Data encryption unscrambles coded data.
3. Storing data in another building or offsite is a form of added security for your data.
4. You can copy any program once you get your hands on it.
5. A hacker is someone who works to detect flaws in a computer program for your benefit.
6. A password can help prevent unauthorized persons from gaining access to your system or files.
7. CDs are indestructible they store information forever.
8. Exposing a diskette to heat and sunlight can damage your diskette.
9. Businesses lose millions of dollars every year because of viruses.
10. Internet fraud occurs mainly when buying or selling products over the internet.

10 marks

Topic: Data Piracy and Integrity

1. In your own words define the term software piracy. 3 marks

2. Explain the four main types of software piracy. 5 marks

3. List four ways to reduce software piracy. 4 marks

4. Identify and explain three methods of unauthorized collection of information.

6marks

5. List four (4) instants of the misuse of information. 4 marks

6. Identify four (4) ways to reduce the misuse of information. 4 marks

7. State four laws from the data protection law. 4 marks

True/False

8. Installing a program on more than one computer is considered software piracy.

9. Software piracy usually result in huge loss of profit for the original owners.

10. If you are caught committing software piracy you can go to prison.

11. Counterfeit is illegally duplicated copies of the sound and its packaging.

12. Online piracy the unauthorized uploading/downloading of copyrighted media to/from a website.

35 marks