Threats to data and protection from attack

Threats: accidental and malicious damage

- Accidental damage: accidental loss of unforeseen data.
- Malicious damage: data loss due to deliberate damage.

Types of accidental damage

- Accidentally overwriting a file or deleting a folder. This will either delete or replace data.
- Forget saving a change to data.
- A program error that causes data loss / data corruption so that it can no longer be read.
- Data input error causing processing error.
- Leave a laptop or storage device on the train.
- Power cuts.
- Natural disasters e.g. floods and fire.

Types of malicious damage

- Dissatisfied employee deliberately removes or corrupts data.
- Attack by malware, which can be viruses, spyware, trojans, keyloggers.
- Social engineering attacks, phishing.
- Hacking attacks including naked force attacks and dictionary attacks.
- Denial of service attacks (DOS/ DDOS).

Malware

- Means malicious software.
- A term to describe software used to disrupt the operation of a computer. Spyware, viruses, trojans, keyloggers, and worms all come under this definition.

Spyware

- Software installed by opening attachments or downloading infected software.
- Spyware can be used to collect stored data without the user's knowledge.

Social engineering

- Psychological manipulation of people into revealing personal or confidential information.
- A common approach is to use social media to get people to disclose their personal details (e.g. the location of your place of birth, followed by the name of your first pet).
- Another method is to send an email asking you to enter a PIN/ password number into a form, to 'unlock' your account.

Denial of Service attacks

- Prevention of access to systems usually by repeatedly sending huge amounts of messages asking a network or server to authenticate a request that has no valid return address.
- This may be from one computer (DOS), or by using a network of computers, (Distributed Denial of Service Attack or DDOS).

Data Interception and theft / hacking

- Once a hacker has access to a system using any of the above methods, they could operate in a number of ways. Two of these are:
  - ◊ prevent access (by changing passwords etc) and claim a ransom to access back to a computer system
  - ◊ theft of data: e.g. stealing consumers' details until a ransom is received and then giving it back or selling for offenders to use.

Threats to data and protection from attack

Viruses

- A virus is a computer program designed to copy itself repeatedly and to associate itself with other computer programs.
- They are used to modify or corrupt information on a targeted computer system.
- A traditional virus must attach itself to another file, which is called a vector.
- **Worms** are another type of virus – unlike a traditional virus, they do not need to attach themselves to another file.

Trojans

- A trojan is a program that appears to perform a useful function, but also provides a 'backdoor' that enables data to be stolen.

Keyloggers

- Programs that capture any text input (e.g. bank details, usernames, passwords) that are typed on a keyboard.
- Sends these details back to another computer along with details of the program / website currently in use.

Protecting data from attack: Encryption

- Encryption is the process of changing data so that it is in a form that cannot be read.
- A famous method of this is the Caesar Cipher. Here, the letters of any message are moved on or back by a number of letters in the alphabet.
- Encryption can be **symmetric** or **asymmetric**.
- **Symmetric** encrypts faster but is not as secure as asymmetric.
- **Asymmetric** encrypts more slowly but is a more secure than a symmetric system.

Firewalls

- Network security system that monitors incoming and outgoing traffic based on pre-determined rules.
- It can be a software or hardware system.
- Controlling inbound and outbound network traffic, packages of data are analysed to determine whether or not they should be let through.

Antivirus software

- This is a program that monitors activity on a computer system for the signs of virus infection.
- Each virus has its own unique 'signature' that is known to virus protection software and stored in a database.
- Data stored on a computer system is scanned to see if any of the virus signatures within the database exist on the system.