Unit 1 - INFORMATION TECHNOLOGY SYSTEMS
Protecting Data and Information

Unit 1 - INFORMATION TECHNOLOGY SYSTEMS

Protecting Data and Information

Contents

Unit 1 - INFORMATION TECHNOLOGY SYSTEMS

Protecting Data and Information

Privacy and Security

🗁At the back or in your own notes make a distinction between the terms: privacy & security.

Let's consider a window in your home. It provides different functions for you. It allows you to look outside. It lets light into your home. It keeps weather outside. You can open a window. In an emergency, you can use a window as an exit.

A window is also susceptible. Just as you can use it in an emergency as a way out, others can use it as an entrance. To protect against unwanted visitors, you can put bars or a grate in front of the window. This still allows you to keep all the desired functionality the window provides. This is **security**.

Just as you can look out a window, others can look in. Thwarting unwanted eyes from looking in can be tackled by putting a blind inside of the window. This is **privacy**. Obscuring the view inside of your home also provides a little security as intruders may not be able to tell when you are home or see the things you own.

Security provides protection for all types of information, in any form, so that the information's confidentiality, integrity, and availability are maintained.

Privacy guarantees that personal information is collected, processed (used), protected and destroyed legally and fairly.

The two interact together because a security program could require credentials to access a network, after checking these credentials users would be have restricted access to personal information based upon their access rights.

Security and Integrity of data

🗁 At the back or in your own notes describe key considerations for security and integrity of data.

Three key strands exist to this debate:

1] The need to **ensure the correctness and integrity of the data** held by an organisation.

2] The need to **protect against the loss or damage** to corporate data.

3] This has to be planned and **co-ordinated via a policy**, it doesn't happen by chance.

Many organisations store their company's data on computer systems and are obviously heavily reliant on their effective performance. Only when normal operations aren't provided, do they realise how dependent they are. All computer systems are predisposed to some form of failure either minor and temporary, or major.

Threats

At the back or in your own notes describe several common threats to security and integrity of data.

Research and describe examples of malicious software.

Threats to security and integrity of data exist from numerous sources. They may be accidental or malicious.

- hardware failure
- theft
- unauthorised use
- natural disaster
- viruses
- disgruntled employees
- hackers
- accidents
- employee accidents
- malicious software

Countermeasures to threats

- **At the back or in your own notes describe key counter measures to common threats.**
- **Research and describe examples of cryptography.**
- **Research and describe examples of biometric security techniques.**

Countermeasures against these threats (logical and physical)

Physical protection involves the use of physical barriers intended to protect against theft and unauthorised access. The reasoning behind such an approach is extremely simple: if access to rooms and equipment is restricted, the risk of theft and unauthorised access is reduced.

Logical protection includes a number of strategies:

- Standard clerical procedures are necessary such as effective use of verification techniques, so that data is entered correctly. Also, clerical procedures such as not downloading software or files.
- Having the latest versions of your AVS is also sound logical protection.
- There should be a policy with regards to 'passwords'. They should be regularly changed, encouraged to be 'strong' and not shared with other members of staff.
- The organisation should organise access rights to their system. These access rights will ensure appropriate access to data so that it might only be read-only or read-write.
- A number of processes are used by organisations such as biometric security. This includes: including iris/retina scans, fingerprint recognition, face recognition, voiceprint recognition.

  For example, an authorised person's fingerprints are captured, digitised and stored so that they can be recalled for comparison. On attempted entry to a system, the user's fingerprints are captured and digitised. These are then compared against the stored versions. If there is a successful comparison/match, then entry to the system is permitted.

This process of comparison against stored digitised data described above works with all biometric techniques. There is an original capture and storage. Each new access to a system requires the same capture but then comparison to the stored data.

- Using encryption on the company's data.
- Ensuring the company's backup policy is followed. Storing the backups in a safe place and checking that they have been conducted properly.
- Storing archived data off-site

Considering on-line systems

Research and describe the use of transaction-logs.

Research and describe the use of record-locking.

- Maintaining security and integrity with on-line systems requires special attention to access rights and passwords. Added to this the company will need to use record-locking. Here, one user who is editing a record (for example making a booking) has sole access to the file for the period where the transaction is taking place. Other users will see the effects of the changed data from the previous user – for example a particular seat on a flight not being available.

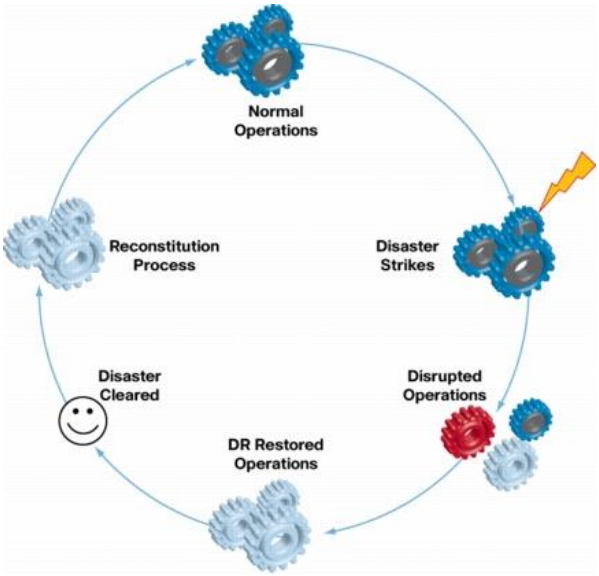
- Other techniques include transaction logging. Here, a special file is created which contains information about each transaction. For example, if a user changes someone's address, a before and after image will be placed in the transaction log (showing a copy of the record before and after the update)

Disaster planning

🗁 **At the back or in your own notes describe the use of a good backup policy and contingency planning.**

Several threats to data have been outline above. One of the countermeasures was to ensure that a good backup policy is followed. A key term here is the **contingency plan**, i.e. how the business can return to normal operations in event of a disaster affecting its operations.

- Many organisations are totally reliant on their data and computer systems. Many don't realise the extent, until they are taken away.
- As already noted, computer systems are liable to some form of failure either minor and temporary, or major.
- Customer confidence needs to be maintained too, because customers may leave to rival businesses if they feel their data and services are being compromised.
- All organisations need to plan for disruption to their operations. This will enable them to recover their data and proceed to operate.



- All organisations are susceptible to a non-zero risk of experiencing unexpected events, whether natural or man-made. Both can lead to internal "disasters" with respect to business operations.
- Consequently, there is a critical need for planning and recovery strategies for the effects of disasters. Disaster recovery plans (DRPs) aim at ensuring that organisations can function effectively during and following the occurrence of a disaster.
- As such, they possess cost, performance, reliability, and complexity characteristics that make their development and execution non-trivial.

Protecting Data and Information

It's not as simple as it may sound, and a number of key elements underpin the planning process:

1] Backups should be planned. The policy should clearly indicate procedures. These backups should also be checked.

2] The policy should indicate the frequency, timing and responsibility.

3] Staff should be trained in recovery procedures including how to successfully restore/rebuild the backed-up data on to the alternative platform. Backups will also have to be executed on this new temporary system too!

4] As referred to above, there should be an alternative computer system.

5] There should be a back-up power supply.

6] Files should be archived off-site.

7] A complex task for any recovery procedure must also be to deal with transactions that were affected/interrupted at the time of the failure.

8] The recovery plan should see that all data is returned as it was before the crisis.

My Answers