Chapter 8: Security Measures
Test your knowledge

Security Equipment

1. **How does biometric security differ from using password security?**

   Biometric security is the use of human physical characteristics (such as fingerprints) to grant access to data. It works on the premise that biometric characteristics are harder to fabricate than a password that is simply typed in. Most users who choose their typed in password, will choose something that is easy to remember and therefore easy to crack.

2. **What are some drawbacks of using swipe cards or smart cards?**

   The drawbacks with swipe cards or smart cards, is that they are easily damaged with magnetic fields and they are easy to forge with the right equipment.

3. **How does a 'security token' work?**

   A security token provides an **authentication code**, which along with an account name and password will grant the user access to sensitive information. The authentication code will change every one to five minutes. This security method is called 'two-factor authentication'.

4. **What ethical issues arise through the use of biometrics?**

   Most biometric systems will keep a copy of your biometric characteristics in their password database. Unauthorised people could get access to your biometric characteristics and use them for malicious purposes.

5. **What does 'two-factor authentication' mean?**

   Two-factor authentication is when there are **two strategies to authenticate** the end user. Most systems only have one-factor authentication (account name and password). Some organisations use security tokens for their second authentication, or a network administrator might use the MAC address of your computer as another authentication method.

6. **Explain how computer equipment can be protected from power fluctuations.**

   Computer equipment can be protected by power fluctuations by using an UPS (interruptible power supply). A UPS will ensure that computer equipment is protected against power spikes by providing a constant current. A UPS can also be used to protect against data corruption by providing equipment with 10 to 30 minutes of power to shutdown in the event of a complete power failure.

7. What is fault-tolerant system?

A fault- tolerant system will continue to work even when a component of hardware has failed. The tolerance is achieved by running multiple components in parallel. For example: A server might have two hard drives, processors or power supplies. Technicians can repair this equipment without interrupting its basic operation.

8. How does a RAID array protect data?

A RAID (Redundant Array of Inexpensive Disks) array is when data is spread over a number of hard drives, so that if one hard drive fails, the others can piece together the missing data and rebuild the files using error-checking codes. Most network servers will have a RAID setup to protect against data loss.

9. List three common backup devices?

- Magnetic Media such as another hard drive (external) or Magnetic tape.
- Optical Drives such as CD-ROMS or DVD's.
- Solid-State storage devices such as USB Keys.

The backup device that you will use will depend on the type of data you are backing up and whether it is a personal or organisational backup.

10. List the different types of backup media.

Students should make a distinction between backup **devices** and backup **media.**
List of backup media:

- Floppy disks
- Super Disks
- Jaz disk
- Hard Disks
- Magnetic Tapes
- CD-ROMs
- DVD's
- USB Key

11. What are some drawbacks of using optical drives for backups?

Although Optical discs are more flexible than tape drives they only have a finite amount of space. If you are backing up any more than 700Mb onto a CDROM or 9Gb onto a DVD, then you need to break up your backups over a number of disks. Compared with Tape Backup systems, an optical disc solution can be quite expensive.

Most DVD's or CD's purchased are easily scratched and not necessarily "archive quality".

12. What are some common methods of surveillance that can be used to protect data?

- Packet sniffers
- Desktop monitoring programs
- Log files
- Closed circuit television (CCTV)
- Telephones

13. How can log files be used to increase the security of data?

On networks, **log files** are kept of users who log in and any files that they access, transfer or try to modify. Analysis of these files can sometimes reveal inappropriate behaviour, or someone using an account that wouldn't be normally accessed due to someone being on holiday or home sick.

14. Explain the purpose of an audit trail.

An audit trail would include log files of system logins, both successful and unsuccessful, as well as any files that were accessed, modified or copied. An audit trail can be constricted by linking the various logs or recording system activity. It is possible to detect patterns of activity and also link specific actions to individual users.

15. How can computer equipment be physically protected?

Computer equipment can be physically protected by keeping it in a locked room and backup discs can be kept in a lockable disk box or in a safe. Security cables can be used to lock down equipment (desktops, notebooks or printers) to a desk.

16. Briefly explain how public key encryption works.

Encryption of data is the process of converting plaintext into cipher text by using an algorithm to make it appear as meaningless jumble to anyone who receives it who is not an authorised recipient. Public key encryption is when the sender uses receiver's public key to encrypt a message or document. Then the receiver uses his or her private key to decrypt the message so as they can read it.

17. What is the purpose of network policies?

Network policies are in place to ensure that users can only gain access to the files that they need, and restrict them from others that they shouldn't use. An example of this would be a school network where students can only see their own files and not the files belonging to staff members.

List three examples of a good password.

A good password should be a combination of letters and numbers and should be at least six characters in length. Students should be able to provide three examples of passwords meeting this criterion.

18. How can network policies help users to choose a good password?

Network policies can restrict the type of password that a user chooses and make them change their password regularly. Sites such as hotmail can inform users as to how 'crackable' or secure their passwords are by running them through an algorithm before accepting them into the system.

19. Why would a firewall be used to protect data?

A firewall is used to **restrict access** to a network from outsiders by using hardware and software that will only allow authorised network traffic to pass through the 'gate' that the firewall protects.

20. How does anti-virus software work?

Anti-virus software detects the presence of viruses when the computer boots up, when a file is executed, when documents are accessed, when files are copied or when they are downloaded from the internet. Anti-virus software scans files for virus signatures or for virus like activity.

Security procedures

1. Explain how a procedure can assist with securing data.

An organisation can prevent data loss by employing correct procedures when storing, communicating or disposing of data. A procedure can reduce the chance of user error by providing guidelines in data handling. For example: If a procedure involves saving (storing) all files to a network drive, then the system administrator can restrict access to these files.

2. What is a 'communication policy'?

The use of email and faxes within an organisation is generally governed by a communication policy. A communications policy lists a set of procedures that employees should follow when using email or faxes.

For example: Each email should have a subject headings, message priority set properly, a signature of the person sending the email and perhaps even a privacy disclaimer. For years organisations have had similar procedures to govern the use of faxes.

3. **What is a PDF document?**

   PDF stands for **Portable Document Format**. It takes a document produced in any package on any platform, and then it turns it into a PDF which maintains the formatting and layout of the original document.

4. **How does a file-naming convention enhance data security?**

   File-naming conventions enhance data security by providing a convention for saving and storing files. When files are organised and named properly it is very easy to see if anything is missing and it is easy to retrieve files if needed.

5. **Give an example of a good and bad filename.**

Bad filename:	Document1.doc
Good filename:	Newsletter 2006-11-v3.doc

6. **What is the difference between a sequential and variation file-naming convention?**

   A sequential file-naming convention clearly shows the date of the last edit. For example: Newsletter 2006-11 03Oct.doc, the next filename would be Newsletter 2006-11 04Oct.doc. Filenames follow a **sequence**.

   A variation file-name convention, shows the version of the file. For example: Newsletter 2006-11-v1.doc, Newsletter 2006-11-v2.doc, Newsletter 2006-11-v3.doc. Filenames show the version or variation of the file.

7. **What is the difference between a full and differential backup?**

   A full backup copies every file from a device to a storage medium (tape backup, DVD, mirrored server). A differential backup only copies those file that have been changed since the last full backup.

8. **What information is entered into a backup log?**

   A backup log shows a summary of a backup routine. It should include:
   - the workstation, system or server name that is backed up,
   - the software used,
   - the number, type and storage location of the backup media,
   - the date of the individual backups,
   - a list of files and folders to be backed up,
   - the type of backup performed.

9. What information is contained in a restoration log?

A restoration log should include:

- the workstation or system restored,
- the date of restoration,
- a list of files and folders restored,
- the backup media used (including date and volume name or number), and
- the reason for the restoration.

10. Why would an organisation need a backup strategy?

An organisation needs a backup strategy to safe guard their data and minimise disruptions in the event of data loss.

11. Explain how the grandparent-parent-child backup routine works.

The most recent copy of the file is called the ‘child’. The following day or week when the second backup is made, the ‘child’ copy becomes the ‘parent’ and there is a new child. When the third backup is made, the ‘parent’ copy becomes the grandparent, the ‘child’ copy becomes the ‘parent’ and there is a new ‘child’.

At any point in time the parent backup is the second oldest copy of the file, the child is the most recent copy of the file.

12. Why is it important to think through the location of backup files?

Backup files are generally needed when data loss occurs. Restoration of files lost needs to occur quickly to prevent productivity loss within an organisation.

Whilst it may be convenient to locate backup files in a central area, the backup strategy needs to take into account the vulnerability of the location of backup files in the event of a disaster such as a fire, huge flood or an earthquake. Most small businesses will store backups in the company safe, but it is preferable to have an offsite location as well. Larger organisations might backup their data to a remote server located in a data centre.

13. What is the difference between archive and backup?

Archiving is the process of copying old files to a long-term storage location and then deleting them from the hard drive or server. Backups are generally performed on current or active files.

14. What issues should an organisation consider when disposing of files?

When disposing of files an organisation needs to ensure that any sensitive data is disposed of properly. Throwing an old backup tape or DVD into the office bin, is probably not the best way of disposing of data as any person can get access to the discarded media once it is collected by rubbish collectors.

Disaster recovery strategies

1. **What is a disaster recovery plan?**

   A disaster recovery plan is a document that tells an organisation what steps are needed to restore the company operations, including computing in the event of a disaster (see Chapter 7).

2. **What are the four key parts of a disaster recovery plan?**

   Four key parts are Emergency plan, Backup plan, Recovery plan and Test plan.

3. **What is the difference between a backup and emergency plan?**

   A **backup plan** covers the procedures that the company is to follow for using and managing backups to restore computer systems and an **emergency plan** explains specific steps to be taken in the event of a natural disaster.

4. **Why is it important to test your disaster recovery plan?**

   Many organisations create backups but never test them to ensure that data can be restored in the event of a disaster. It is important for system managers to test their disaster recovery plan to ensure that operability **can** be restored in the case of a disaster.

5. **What is a disaster simulation?**

   A disaster simulation is similar to a ‘fire drill’ that you might regularly participate in a school or business. During a disaster simulation, each staff member carries out their assigned procedures. If there are any problems with the disaster plan, they should be identified and corrected during testing. Ideally a disaster recovery plan should be carried out without warning to ensure that procedures work correctly.

Evaluation of file-management strategies

1. **How can you evaluate the integrity of data that must be reliable and accurate?**

   Evaluating the integrity of data consists of developing evaluation criterion that will allow you to judge the effectiveness of data accuracy, reliability and timeliness.

   For example: Evaluating reliability might consist of repeatedly saving files and testing for corruption of data. See figure 8-21

2. **What security aspects would tell you if file-management strategies were successful?**

   File Management strategies should be introduced into an organisation to ensure that data is kept secure and also accessible. Evaluating the effectiveness of security aspects for data loss would tell you if file-management strategies are successful.

3. **Why is ease of retrieval an important criterion?**

   Ease of retrieval of files depends on proper observance of folder and file-naming conventions, and the correct use of file extensions.

   If employees cannot retrieve files efficiency (minimal time, minimal effort), then it may impact on their effectiveness (quality and timeliness) within the workplace.

4. **How could the currency of files as an effective file-management strategy be assessed?**

   The currency of files should be evaluated to ensure that the most recent possible versions of files are available when needed. Files should be regularly checked for currency and archival procedures introduced to ensure that old files are properly archived or disposed of.