UNIT 19

Data Security 2

STARTER **1** Consider these examples of computer disasters. How could you prevent them or limit their effects? Compare answers within your group.

1 You open an email attachment which contains a very destructive virus.
2 Someone guesses your password (the type of car you drive plus the day and month of your birth) and copies sensitive data.
3 Your hard disk crashes and much of your data is lost permanently.
4 Someone walks into your computer lab and steals the memory chips from all the PCs.
5 Your backup tapes fail to restore properly.

READING **2** Study this table of security measures to protect hardware and software. Which measures would prevent or limit the effects of the disasters in Task 1?

Control Access to Hardware and Software

* Lock physical locations and equipment.
* Install a physical security system.
* Monitor access 24 hours a day.

Implement Network Controls

* Install firewalls to protect networks from external and internal attacks.
* Password-protect programs and data with passwords which cannot easily be cracked.
* Monitor username and password use - require changes to passwords regularly.
* Encrypt data.
* Install a callback system.
* Use signature verification or biometric security devices to ensure user authorisation.

Protect against Natural Disasters

* Install uninterruptible power supplies and surge protectors.

3 Find words or phrases in the table which mean:

1 copies of changes to files made to reduce the risk of loss of data
2 software available for a short time on a free trial basis; if adopted a fee is payable to the author
3 cannot be disrupted or cut
4 put at risk
5 deciphered, worked out
6 protect data by putting it in a form only authorised users can understand
7 a combination of hardware and software to protect networks from unauthorised users
8 observe and record systematically
9 measuring physical characteristics such as distance between the eyes
10 at regular intervals

Backup Data and Programs

* Make incremental backups, which are copies of just changes to files, at frequent intervals.
* Make full backups, which copy all files, periodically.
* To protect files from natural disasters such as fire and flood, as well as from crimes and errors, keep backups in separate locations, in fireproof containers, under lock and key.

Separate and Rotate Functions

* If functions are separate, then two or more employees would need to conspire to commit a crime.
* If functions are rotated, employees would have less time to develop methods to compromise a program or system.
* Perform periodic audits.

Protect against Viruses

* Use virus protection programs.
* Use only vendor-supplied software or public domain or shareware products that are supplied by services that guarantee they are virus-free.

LANGUAGE WORK Cause and effect (2) links using allow and *prevent*

What is the relationship between these events?

1 The scanner finds a match for your fingerprint.
2 The keyboard is unlocked.
3 You can use the PC.

1 and 2 are cause and effect. We can link them using the methods studied in Unit 18. In addition we can use an *if*-sentence. Note that the tenses for both cause and effect are the same. For example:

If the scanner finds a match for your fingerprint, the keyboard is unlocked.

2 allows 3 to happen. We can link 2 and 3 using *allow* or *permit.*

The keyboard is unlocked, *allowing/permitting* you to *use* the PC.

What is the relationship between these events?

4 The scanner does not find a match for your fingerprint.
5 The keyboard remains locked.
6 You cannot use the PC.

We can show that 4 and 5 are cause and effect using the methods studied in Unit 18. We can also use *therefore.*

The scanner does not find a match for your fingerprint, *therefore* the keyboard remains locked.

5 prevents 6 from happening. We can link 5 and 6 using *prevent* or stop.

The keyboard remains locked, *preventing* you *(from) using* the PC.
The keyboard remains locked, *stopping* you *(from) using* the PC.

4 Put the verbs in brackets in the correct form in this description of how smart cards work.

Smart cards prevent unauthorised users .....[1] (access) systems and permit authorised users .....[2] (have) access to a wide range of facilities. Some computers have smart card readers .....[3] (allow) you .....[4] (buy) things on the Web easily and safely with digital cash. A smart card can also send data to a reader via an antenna .....[5] (coil) inside the card. When the card comes within range, the reader's radio signal .....[6] (create) a slight current in the antenna .....[7] (cause) the card .....[8] (broadcast) information to the reader which .....[9] (allow) the user, for example, ...[10] (withdraw) money from an ATM or .....[11] (get) access to a system.

5 Decide on the relationship between these events. Then link them using structures from this and earlier units.

1 Anti-virus program
- a A user runs anti-virus software.
- b The software checks files for virus coding.
- c Coding is matched to a known virus in a virus database.
- d A message is displayed to the user that a virus has been found.
- e The user removes the virus or deletes the infected file.
- f The virus cannot spread or cause further damage.

2 Face recognition
- a You approach a high-security network.
- b Key features of your face are scanned.
- c The system matches your features to a database record of authorised staff.
- d Your identity is verified.
- e You can log on.
- f Your identity is not verified.
- g You cannot use the system.

3 Voice recognition
- a Computers without keyboards will become more common.
- b These computers are voice-activated.
- c The user wants to log on.
- d She speaks to the computer.
- e It matches her voice to a database of voice patterns.
- f The user has a cold or sore throat.
- g She can use the system.
- h Stress and intonation patterns remain the same.

PROBLEM-SOLVING 6 Study these illustrations for two forms of security scanning. Write your own captions for each of the numbered points.

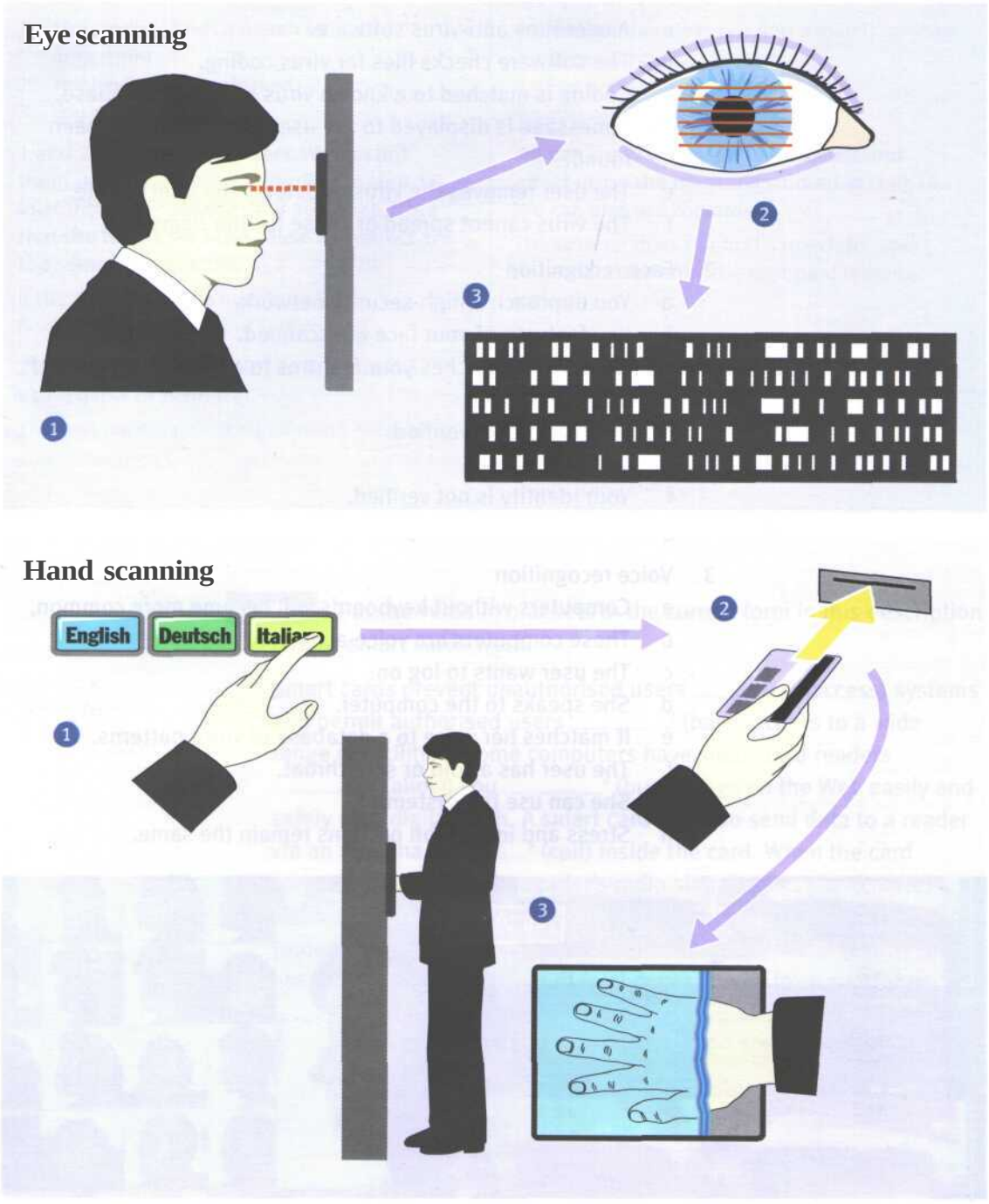

Fig 1
Scanning technology

SPEAKING **7** **Backups** Work in pairs, A and B. You each have details of one form of backup. Explain to your partner how your form of backup works. Make sure you understand the form of backup your partner has. Ask for clarification if anything is unclear.

Student A Your information is on page 188.
Student B Your information is on page 194.

WRITING **8** **Firewalls** Study this diagram of a firewalled network system. Write a description of how it operates. You may need to do some research on firewalls to supplement the diagram. Your description should answer these questions:

1 What is its function?
2 What does it consist of?
3 How are the firewalls managed?
4 How does it control outgoing communications?
5 How does it prevent external attack?

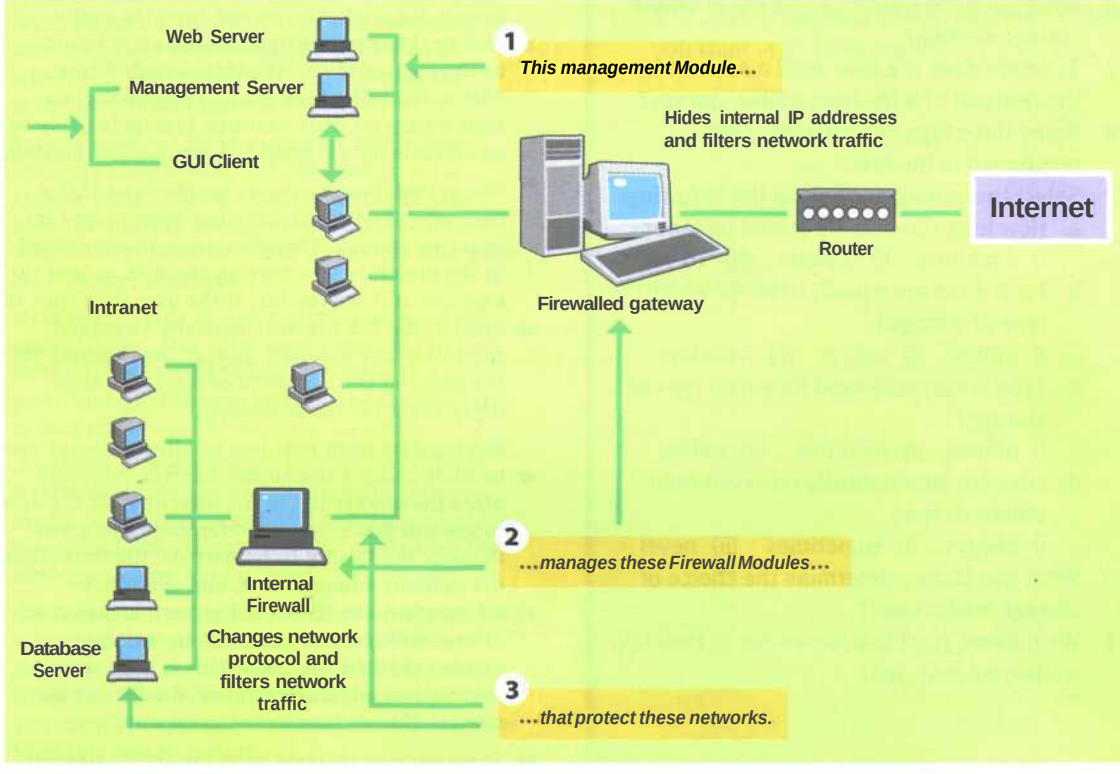

Fig 2
How a firewall works

SPECIALIST READING

A Find the answers to these questions In the following text

1 What factor determines which type of storage is used to store a file in an HSM system?
2 Complete the following table using information from the text.

Storage Type	Media	Speed
offline	optical	very fast with quickest access speed

3 What happens to data that is not accessed for a long time?
4 How does the system record that a file is in near-line storage?
5 What happens when a user tries to access a file in near-line storage?
6 What does the reference to a file in offline storage contain?
7 To whom does the user send a request for the retrieval of a file from offline storage?
8 Name three types of magnetic tape mentioned in the text.
9 Select the correct answers in the following:
a How long can data be stored on tape?
i) 6 months ii) 2 years iii) 10 years
b Hard disks are usually used for which type of storage?
i) offline ii) online iii) near-line
c Tape is normally used for which type of storage?
i) offline ii) near-line iii) online
d Files are automatically retrieved from offline storage
i) always ii) sometimes iii) never
10 What two factors determine the choice of storage media used?
11 What items must you remember to maintain while data is stored?

Backup HSM and Media Choice

Near-line and offline storage (often called Hierarchical Storage Management) is the modern way of dealing with current storage needs. Hard disks are becoming cheaper, but data storage requirements are higher, so it's better to plan for HSM than assume disks can continually be added to systems.

HSM is essentially the automatic movement of data between media, the media type used depending on when it was last accessed. Many software and hardware vendors have HSM solutions, and all are based on the same basic techniques.

The most common HSM setup is where there's online storage (the hard disk), near-line storage (some sort of fast media from where a file can be quickly retrieved), and offline storage (slower media that might take some time for files to be recovered, but it is cheaper for a long-term storage). This arrangement is the major thrust of today's systems. Most of the time these systems will comprise optical media for near-line and tape media for offline storage.

Data is automatically moved from the online disk to the near-line optical media if it hasn't been accessed for a definable period of time. This is typically three months (depending on your business). This near-line system is likely to be erasable optical disks in some form of jukebox.

The system has to operate on the basis that a user won't know that a file has been moved into near-line storage. Therefore some marker is left in the directory structure on the disk so that the user can still see the file. If the user then tries to open it, the file will automatically be copied from near-line to online storage, and opened for the user. All the user notices is a slight time delay while the file is opened.

Moving data from near-line to offline storage can be done using a similar mechanism, but more often the marker left in the directory for the user to see will just contain a reference. This gives the user the facility to request the file back from the systems administrator, and could have information like 'This file has been archived to offline media' and a reference to the tape number that the file is on. This is then sent to the systems administrator and the file can be recovered from tape in the usual way.

Some modern systems have the ability to keep multiple tapes in a tape changer or jukebox

system, so retrieval from offline to online storage can be automatic. However, it is more likely that when a file goes into offline storage it will never be recovered, as it has probably been untouched for several months (again depending on the business). Therefore the requirement to recover from offline to online is reasonably infrequent.

The choice of storage media type is a crucial aspect of HSM. The cheapest is undoubtedly tape (be it digital, analogue or digital linear), so this tends to be used for offline storage. However, tape has no guarantee of data integrity beyond one or two years, whereas optical systems, such as CDs, WORMs and MO disks, have much better data integrity over a longer period of time. Depending on the precise application, archiving systems are usually based on the media type that has the best integrity. The major suppliers within the HSM market are totally open about the media that can be used with their software. Current HSM systems support most hardware devices, so you can mix and match media to suit requirements. Given the fact that media choice depends on the length of time you want your data to remain intact, and also the speed at which you want to recover it, the choice for many system managers is as follows.

Tape is used for backup systems where large amounts of data need to be backed up on a regular basis. Tape is cheap, integrity is good over the short to medium term, and retrieval from a backup can be made acceptable with good tape storage practices.

Near-line storage should be based on erasable optical disks. This is because access is random, so the access speed to find and retrieve a particular file needs to be fast, and data integrity is also good.

Archiving systems should probably be CD- or WORM-based, as again access speeds are good, media costs are reasonably cheap and, importantly, the integrity of the media over the medium to long term is good.

One important thing to remember with archiving systems is the stored data's format. The data might be held perfectly for 10 or 15 years, but when you need to get it back, it's essential that you maintain appropriate hardware and software to enable you to read it.

[Adapted from 'Backup HSM and media choice' by Phil Crewe, Tape Backup, PC Magazine, May 1996]

B Re-read the text to find the answers to these questions.

1 Mark each of the following statements with True or False:

a Hard disks are still very expensive.
b Near-line storage needs to have a quick access speed.
c Near-line storage is usually some form of jukebox.
d Offline storage needs to have a fast access speed.
e Users are aware that their files have been moved to near-line storage.
f The movement of files between near-line and online storage is automatic.
g The user sometimes has to request files from the systems administrator.
h Files are frequently recovered from offline storage.
I Tape has much better data integrity than optical media.
j It is usually possible to use whatever media you want in an HSM system.