OCR Cambridge Technicals *in* ICT [Level 3]

IT-Year 12- Unit 2- LO6

UNIT 2 LO6 KNOWLEDGE ORGANISER

Understand the principles of information security

6.1 PRINCIPLES OF INFORMATION SECURITY

Confidentiality – information can only be accessed by individuals, groups or processes authorised to do so

Integrity – information is maintained, so that it is up to date, accurate, complete and fit for purpose

Availability – information is always available to and usable by the individuals, groups or processes that need to use it

Confidentiality is a legal requirement, as stipulated in the **Data Protection Act**.

Integrity is 'the maintenance of, and the assurance of the accuracy and **consistency** of **data'** - again the DPA stipulates that once an organisation is in possession of data, they must ensure that these standards apply.

6.2 RISKS

Unauthorised or unintended access to data (e.g. espionage, poor information security policy)

Accidental loss of data (e.g. human error, equipment failure)

Intentional destruction of data (e.g. computer virus, targeted malicious attack)

Intentional tampering with data (e.g. fraudulent activity, hacking)

Availability of information is important - but this should not be at the expense of security. For example, employees should ensure that photocopying is minimised so that there are not additional copies of sensitive data

Most "accidental" data loss, or unauthorised access to data is in fact caused by human error

82%

..of network security breaches reported to the **Information Commissioners Office** are (2018) were caused by human error

6.3 IMPACTS

Loss of intellectual property

Loss of service and access

Failure in security of confidential information

Loss of information belonging to a third party

Loss of reputation

Threat to national security

Recent cases of failures of information security

Intellectual property covers the theft of ideas - for example, product designs, books, music

Service and access means that access to the internet becomes difficult or impossible due to theft of bandwidth, or use of stolen passwords

The impact of the theft of **confidential** information depends on what information was stolen and to whom it belongs.

Some companies - like Yahoo! and Talk Talk suffered very bad publicity (and consequently, a poor **reputation**) due to data breaches.

National Security could be at risk depending on what information is stolen - for example, military secrets, details of troop movements, names of intelligence operatives.

EXAMPLES OF RECENT INFORMATION SECURITY FAILURES

Breach	
Adobe [2013]	Hackers stole 3 million unencrypted user accounts
Canva [2019]	Accounts of 137 million users attacked
Boots [2020]	Approx. 50,000 customer accounts
Virgin Media [2020]	Personal details of 900,000 customers accessed

6.4 PRINCIPLES OF INFORMATION SECURITY

Policies, e.g.:

- staff access rights to information
- responsibilities of staff for security of information
- disaster recovery
- information security risk assessment
- effectiveness of protection measures
- training of staff to handle information

THE IMPORTANCE OF POLICIES

Effective IT policies are important, but only work if they are kept up to date and reviewed regularly. They must be clearly communicated to staff and there needs to be monitoring to ensure that they are followed.

6.5 PHYSICAL PROTECTION

locks, keypads and biometrics used on:

- workstations
- server room access

Placing computers above known flood levels

Backup systems in other locations

Security staff

Shredding old paper based records

PHYSICAL PROTECTION is there to make equipment secure and to stop unauthorised people physically going to the computer and accessing IT systems.

Locks, keypads and biometrics involve a range of measures, including fingerprint and retina scans, electronic locks (with keycards and keypads) and straightforward "manual" locks/keys

Placing computers above known flood levels may not seem to be an important measure, but there are even parts of the UK, where flooding is regular problem. Computer equipment does not survive water damage and there is a real risk of data loss.

Consider… Are there other forms of "physical protection" that organisations can employ? How many data breaches do you think take place, because of a lack of physical protection?

Off-site backup is very important– backing-up data is pointless is if it is vulnerable to fire or flood, and so systems like cloud storage may be used to store data remotely. IT staff might even take tape or disk backups home with them.

Security staff can act as a deterrent for physical attacks on data - but they cannot protect against remote hacks.

Care must be taken with data stored on paper as well as digitally. This means that old or unwanted records must be **shredded** - simply throwing them away is not sufficient.

6.6 LOGICAL PROTECTION

Tiered levels of access to data

Firewalls (hardware and software)

Anti-malware applications

Obfuscation

Encryption of data at rest

Encryption of data in transit

Password protection

LOGICAL PROTECTION means computer-based methods that can be put in place by the network or system administrator

Levels of access can be set, based around the level of authority each user has. For example, files could be set to read-only, for some user while edit-access can be granted to others.

Firewalls can be hardware or software and are used to intercept and monitor **data packets** from both incoming and outgoing network traffic

Consider… with so many methods of preventing data breaches and thefts, why do you think that they continue to take place on such a regular basis?

Anti-malware software can be used to detect threats such as, **spyware**, **viruses** and **Trojans**.

Encryption ensures that data can not be read even if it is intercepted. A key would be needed to **decrypt** the data.

Passwords need to be set using a sensible set of rules to ensure that they are hard to guess.

Obfuscation means making something hard to read or see. Obfuscation measures include the use of * characters to mask password entry, or **X**'s when credit-card details are being entered