Unit 1: Security and data management

Key terms

Term	Definition
Network security	The range of measures that can be taken to protect network data from accidental or malicious damage.
Encryption	Conversion of data, using an algorithm, into cyphertext that cannot be understood by people without the decryption key.
Compression	The process of reducing file size to allow more data to be stored on the disk and increase transfer speeds.
Backup	A copy of data that can be used if the original data is lost.
Archiving	The process of storing data that is not in current use for security, legal or historical reasons.
Cybersecurity	The range of measures that can be taken to protect computer systems from cyberattack.
Cyberattack	An attempt to expose, alter, disable, destroy, steal or gain unauthorized access to data on a computer system or smart device.
Malware	**MAL**icious soft**WARE**; the term used for any kind of computer software written to enable a cyberattack
Vulnerabilities	Software security flaws or holes that are fixed via the release of patches.
Cookies	Data downloaded from a website that allows the website to identify the computer in future.

Network security

Risks to private and confidential data become greater as it is shared across a network.

Measures to control these risks include:

- Limiting levels of access
- Using strong passwords
- Encryption.

Encryption / decryption example using the XOR logical operator

Original Data	10101010		Cyphertext	01011010	
Key	11110000	XOR	Key	11110000	XOR
Cyphertext	01011010		Original Data	10101010	

Network policies

Data/network management will involve acceptable use policies (rules for using a network), a backup policy for making regular backups and creating generations of files, archiving and implementing an effective **Disaster Recovery Plan**, which should cover:

Before: risk analysis, preventative measures and staff training

During: staff response, implementing contingency plans

After: replacing hardware, reinstalling software, restoring data from backups.

Compression and compression types

Lossless compression uses an algorithm that compresses data into a form that may be decompressed without any loss of data.

Lossy compression. Compressing file size by discarding some of the data.

$$\textit{Compression ratio} = \frac{\textit{Original file size}}{\textit{Compressed file size}}$$

Lossy compression is used to compress multimedia data, such as images, sound and video, for internet streaming.

Cybersecurity

Online networks are liable to cyberattacks targeted to access confidential data, such as customers' details. This data is expensive to gather, and its loss could result in loss of reputation and even business failure.

Cyberattacks are carried out using types of malware including **viruses**, **spyware**, such as key loggers, and **trojans**.

Protections against malware

- Install anti-virus software
- Use a firewall
- Keep the operating system up to date
- Use the latest version of browsers
- Look out for phishing emails.

Forms of cyberattack

Shoulder surfing	Using direct observation to get information.
SQL Injection	Injected SQL commands can alter SQL statements and compromise the security of information held in a database.
Denial of Service (DoS)	Making a website and servers unavailable to legitimate users, by swamping a system with fake requests.
Password attacks	Brute force or dictionary attacks to discover passwords.
IP Spoofing	Changing the IP address of a site so that a visitor is taken to a fraudulent or spoofed web page.
Social engineering	Deception such as phishing. Tricking a user into giving out sensitive information.

Identifying vulnerabilities

Footprinting and ethical hacking, including strategies for penetration testing (targeted, internal, external and blind testing).

Secure by design

An approach to make software systems as free of vulnerabilities as possible through continuous testing and adherence to best programming practices.