Component 1: Networking

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.
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.

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 include:

Phishing

Sending fraudulent emails claiming to be from reputable companies in order to scam people to reveal information, such as credit card numbers.

Social engineering

Cyberattacks that take advantage of human vulnerabilities such as trust or habit in order to convince people to take action such as clicking a fraudulent link or visiting a malicious website.

Brute force attacks

Gaining access to a site or server (anything that is password protected) with a view to stealing confidential data, using software to try various usernames and passwords again and again until access is allowed.

Denial of Service (DoS)

Making a website and servers unavailable to legitimate users by swamping systems with fake requests for information.

Date interception and theft

Methods include use of hijacking software that pretends to be the destination for data packets, or use 'packet sniffing' software and hardware to intercept certain packets, such as plain text files containing passwords and set-up information.

SQL Injection

Entering malicious code in SQL statements, via web page input that will allow access to data stored in a database.

Protecting against threats

(during design, creation, testing and use)

Penetration testing, or ethical hacking, the practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit.

Network forensics involves the monitoring and analysis of network traffic to gather legal evidence or identify sources of intrusion.

Anti-malware software protects computers from malware such as spyware, adware, and viruses. Files that exhibit suspicious behaviour are flagged and isolate or sandboxed for further analysis and then removed if a threat.

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.

Double authentication. A security process requiring users to provide two different authentication factors, such as an ID code and letters from a secret word.

Encryption. A process that encodes a message or file so that it can be only be read by authorised people. Encryption uses an algorithm to scramble, or encrypt, data and then uses a key for the receiving party to unscramble, or decrypt, the information.

Encryption / decryption example using the XOR logical operator					
Original Data	10101010		Cyphertext	01011010	
Key	11110000	XOR	Key	11110000	XOR
Cyphertext	01011010		Original Data	10101010	