J836 – Cambridge Nationals Level 1/2 Information Technologies

R050 – IT in the Digital World

TA4: Cyber-security and legislation

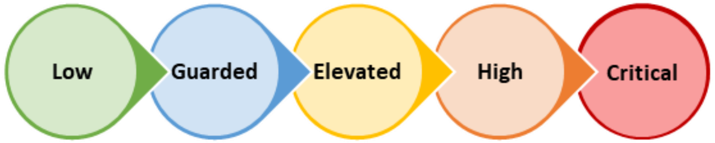
4.1. Threats

Types of threats	
Cyber-security	The practice of defending digital devices, including computers, servers, mobile devices, electronic systems, networks and data, from malicious attacks
DoS	(**Denial of Service**) An attempt to make a digital system, for example a network or website, unavailable to its users by flooding it with network traffic.
Hacking	Hacking means finding a weakness in an established system and exploiting them
Malware	(**Malicious Software**) Malware is installed on a computer system and collects information about users without their knowledge
Social engineering	The art of manipulating people so that confidential information can be found out

Hacking	
Black Hat Hacking	The hacker hacks into the computer system with malicious intent. The intent can include theft, exploiting the data stolen or seen, and selling the data on. Black hat hackers carry out illegal hacking activities and can be prosecuted.
Grey Hat Hacking	The hacker hacks into the computer system for fun or to troll but does not have malicious intent towards the computer system. If they find a vulnerability, they offer to fix it – but for a fee. They can manipulate rankings of website in a search engine.
White Hat Hacking	The hacker is given permission to hack into systems to identify any loopholes or vulnerabilities. White hat hackers are motivated to keep the computer systems as safe as possible from malicious hacking attempts.

Malware	
Adware	Advertising-supported software which generates revenue for its author
Botnet	A botnet, and the person who created it attempts to take control of digital systems
Ransomware	Holds a computer system captive and demands a ransom, usually money, to release it
Spyware	Spyware can collect data from an infected digital system, including personal information like websites visited, user logins and financial information
Trojan horse	A standalone malicious program designed to give full control of an infected digital system to another digital system
Virus	A virus attempts to make a computer system unreliable
Worm	A standalone computer program that replicates itself so it can spread to other computers

Cyber Security Threat Levels:



Social engineering					
Baiting	Tries to get victims to give cybercriminals the information they need with promises of goods in return.	Phishing	Tries to get users to input their credit or debit card numbers, or security details or log-in details, into a fake website.	Quid pro quo	Tries to disable anti-virus software so that software updates, usually malware, can be installed to gain access to a digital system.
Shoulder surfing	Aims to steal data or information by overseeing what an individual is viewing/typing.	Scareware	Tries to scare people into downloading and buying useless software.	Pretexting	A cybercriminal lies to get data or information.

J836 – Cambridge Nationals Level 1/2 Information Technologies

R050 – IT in the Digital World

TA4: Cyber-security and legislation

4.2. The impacts of a cyber-security attack on individuals and/or organisations

Data Destruction	Data is destroyed by a cyber-security attacker and no longer exists. ***E.g.*** *Attacker deletes customers' orders.*
Data Manipulation	Data is edited, usually to meet the needs of the cyber-security attacker. ***E.g.*** *Attacker changes the data in a news feed on social media platforms.*
Data Modification	It changes data to meet the needs of the attacker. However, the attacker usually has different aims and the crime may not be found for a long time. ***E.g.*** *Attacker changes the amount of money in a bank account and the increased amount of money.*
Data Theft	Cyber-attacker steals computer-based data from a person or organisation, with the intent of compromising privacy or obtaining confidential information. Can occur when the data is at rest or in transit.
Data at rest	The data is not moving from device to device or network to network. The data is stored on, for example, a hard drive, laptop, flash drive or archived by an organisation.
Data in transit	The data is being sent to two or more authorised users, or moving, from one location to another, for example across the internet or through a private network.
Identity theft	When personal details are stolen.
Identity fraud	When personal details are stolen and used to commit fraud. ***E.g.*** *Take out a loan in someone else's name.*

4.3. Prevention measures

Physical prevention measures

Usually hardware based. The aim is to stop unauthorised access to digital devices, and the data and information stored on them.

Biometric devices	Devices which use a physical characteristic of the user, such as a fingerprint, eye scan or voice, which needs to be positive match before the device can be accessed.
Keypads	A type of lock where the correct code must be inputted before the lock opens.
RFID	(**Radio-frequency Identification**) Access badges or tags that use radio frequency to transfer data from the tags to a digital system, for example to allow access to a room.

Logical prevention measures

Software based techniques used to authenticate a user.

Access rights and Permissions	Control over who has access to a digital system, folder, files, data and/or information.	2FA	(**Two-factor Authentication**) A process to verify a user logging into their account by receiving a token via an authorised method and entering this token to gain access.
	A set of attributes that can be set to determine what a user can do with files and folders. E.g. read, write, edit, delete.	Encryption	The process of encoding files or data.
Anti-virus/ malware software	Security software which are designed to prevent, detect and remove viruses and other malware.	Asymmetric encryption	(**Public key encryption**) The encryption key is available to anyone to encrypt data but only the person who receives the data receives the decryption key.
Manual updates	Users manually prompt for the update to occur.	Symmetric encryption	This is when the encryption and decryption keys are the same.
Automatic updates	Some software updates occur automatically. This process is usually completed in real time.	Firewalls	A security device that mitigates against threats by examining data packets. Can be a hard/software - both work in the same way.
Usernames and passwords	The username acts as authorisation whilst the password acts as authentication. Without both parts being correct, access will be denied.	Secure backups	A copy of the data/files that are currently in use. Backups are made regularly and stored away from the digital system, preferably in another building in a secure place.

J836 – Cambridge Nationals Level 1/2 Information Technologies

R050 – IT in the Digital World

TA4: Cyber-security and legislation

4.3. Prevention measures

Secure destruction of data	
Data sanitation	The process of deliberately, permanently and irreversibly removing or destroying the data stored on a storage device to make the data unrecoverable. **E.g.** *Data erasure, Magnetic wipe, Physical destruction.*
Data erasure	Software used to overwrite the data on a storage device.
Magnetic wipe	When the magnetic field part of a storage device is removed. This makes all the data stored on the storage device unreadable.
Physical destruction	Physical destruction of a storage device is the most secure. The device is so thoroughly destroyed that the data cannot be retrieved. Methods can include: hard drive shredder, steamroller, burning, drill through or hammer on the device.

4.4. Legislation related to the use of IT systems

Computer Misuse Act (CMA)	
Purpose	Protect data and information that is held on computer systems. The CMA relates to illegal access to files and data stored on digital systems.
Main parts to the act:	1. Unauthorised access to computer material 2. Unauthorised access with intent to commit or facilitate the commission of further offences 3. Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of a computer 4. Making, supplying or obtaining any articles for use in a malicious act using a computer 5. Unauthorised acts causing, or creating risk of, serious damage

Data Protection Act (DPA)	
Purpose	Attempts to control how personal data and information are used by organisations and the UK Government. The Act also gives data subjects control of their personal data.
Main principles:	1. Used fairly, lawfully and transparently 2. Used for specified, explicit purposes 3. Used in a way that is adequate, relevant and limited to only what is necessary 4. Accurate and, where necessary, kept up to date 5. Kept for no longer than is necessary 6. Handled in a way that ensures appropriate security, including protection against unlawful or unauthorized processing, access, loss, destruction or damage

Copyright, Designs and Patents Act (CD&PA)	
Purpose	Establishes copyright to protect the creative work of individuals or businesses. The CD&PA aims to protect intellectual property.
Main parts to the act:	1. Illegal download of video/audio files 2. Software piracy, wither by illegal download or illegal distribution 3. Theft of intellectual property, for example text/written work, including on websites 4. Use of software without the relevant license 5. Using/downloading images without permission of the copyright holder

Health and Safety (H&S) at Work Act	
Purpose	Provides guidance to employers and employees about health and safety at work. The part of the act that applies to people working with digital systems is the Health and Safety DSE Regulations.
Main tasks:	1. Analyse workstations and assess and reduce risks 2. Plan work so that there are breaks or changes of activity 3. Arrange and pay for eye tests and glasses (if special ones are needed) 4. Provide health and safety training and information

Freedom of Information Act (FoI)			
Purpose	The Act deals with access to official information and people being able to find out any information on any topic from any public authority, i.e. right of access.	**Provides access to:**	1. Official information 2. Any information on any topic from any public authority (except for information regarded as “exceptions”)