

Unit 11 Cyber Security Glossary Of Terms

Learning Aim A – Cyber Security Threats

Key term	Definition	References
Malware	A type of software program that are designed to cause problems or damage to a computer system.	https://searchsecurity.techtarget.com/definition/malware
Spyware	A type of Malware that sits on a computer system and records everything a user is doing. A typical Spyware program is a Keylogger which will record everything a user types on their keyboard.	https://www.kaspersky.co.uk/resource-center/threats/spyware
Adware	A type of Malware that causes adverts to pop up randomly. This type of malware is not malicious, but merely annoying.	https://www.malwarebytes.com/adware/
Ransomware	A type of Malware that encrypts all data within a computer system. Data will only be unencrypted if an organisation pays a substantial ransom. Ransomware attacks have become more frequent since 2020 and is seen as very big business for Cyber Criminals.	https://securelist.com/ransomware-world-in-2021/102169/
Virus	A virus is a type of Malware (or program) that has the specific aim of infecting a computer system to do some form of damage and then to spread itself through the system.	https://uk.norton.com/internetsecurity-malware-what-is-a-computer-virus.html

All text copyright © TheComputingTutor 2020. All rights Reserved.



Worm	A type of virus that will leave a copy of itself on the target computer before making copies of itself and spreading through a System. A worm will typically try to use network protocols to infect other computers.	https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html
Rootkit	A type of virus designed to get access to the most secure parts of your computer Operating System . Rootkits can remain very active, but hidden. They can give attackers full remote access to your computer	https://us.norton.com/internetsecurity-malware-what-is-a-rootkit-and-how-to-stop-them.html
Trojan	A Type of virus that hides inside a legitimate piece of software e.g. a VB macro inside a Word Document. When a user opens the legitimate file, the virus code is triggered. Trojans are used to penetrate Firewalls as the virus looks like a normal document.	https://www.kaspersky.co.uk/resource-center/threats/trojans
Hacking	This is the process of finding weaknesses in a network defences in order to gain unauthorised access to the system. Hacking a system may not necessarily result in damage to any data.	https://www.avg.com/en/signal/what-is-hacking
Sabotage	The process of deliberately breaking or damaging a network or system, usually by a person or organisation with relationship to the target.	
Social-Engineering	This is where people are manipulated in order to disclose confidential information. This could involve sending phishing texts or emails to a person to get them to divulge a password; it could involve an attacker pretending to be a trusted friend on a social media site and convincing the target to give up their bank details.	https://www.webroot.com/gb/en/resources/tips-articles/what-is-social-engineering



Operational Loss	This is when a business or organisation is not able to carry out its day-to-day tasks as a result of a Cyber Security Incident.	https://lifars.com/2020/04/operational-and-cyber-risks-in-the-financial-sector/
Financial Loss	This is when a business or organisation loses money / income / profit because of a Cyber Security Incident. This could be as a result of operational loss.	https://cybersecurityventures.com/hacke-rpocalypse-cybercrime-report-2016/
Reputation Loss	This is when customers or other organisations lose trust and confidence in a business or organisation because of a Cyber Security Incident. This could be because data confidential has been lost or stolen and Customers do not trust the organisation to keep their data secure.	https://ivision.com/blog/reputation-risk-management-cybersecurity/
Intellectual Property Loss	This is when a business or organisation loses anything that was created by them because of a Cyber Security Incident. This could be program source code, designs, images, videos or audio files.	https://www.gov.uk/intellectual-property-an-overview
Cyber Security	This is the application of processes and hardware and software technologies to protect systems and networks as well as the data they contain from attack by a third party.	https://www.kaspersky.co.uk/resource-center/definitions/what-is-cyber-security



Learning Aim A – System Vulnerabilities

Key term	Definition	References
Firewall	A system (usually a combination of hardware or software) that is designed to monitor and block traffic coming into as well as out of the network .	https://www.cisco.com/c/en_uk/products/security/firewalls/what-is-a-firewall.html
Firewall Port	A port in a Firewall can mean either the physical socket where a cable is plugged in, or a 'port number' which can refer to a specific service inside your computer network . Common service ports are 80 (HTTP), 443 (HTTPS) and SMTP (25).	https://www.watchguard.com/uk/wgrd-resource-center/security-fundamentals/what-is-a-port
External Storage Device	A device connected to your computer that is not inside the machine but stores files and data. These could be external USB hard drives, or Network Access Storage (NAS) drives.	https://uk.pcmag.com/nas/14710/the-best-nas-network-attached-storage-devices
File Permissions	A set of rules that determine what actions a user can perform on a file. Typical actions include Read, Write, Update or Delete. Permissions can be assigned to individual users or groups of users e.g., Staff or Student user group in your school.	https://websitebuilders.com/how-to/glossary/file_permissions/



Password Policy	A set of rules that determines what passwords should look like and how they should be maintained e.g., a password must be longer than 8 letters and must be changed every month.	https://www.ncsc.gov.uk/collection/passwords/updating-your-approach
SQL Injection	SQL injection is where a malicious attacker enters some SQL code into a form field on a web page. When the page is submitted to the server, the server reads the input and executes the SQL code against a database.	https://www.w3schools.com/sql/sql_injection.asp
Zero Day Exploit	A brand-new system vulnerability that has been identified by hackers for which no fix yet exists and has been attacked immediately. The vulnerability is used before a fix is made available.	https://www.kaspersky.co.uk/resource-center/definitions/zero-day-exploit
Operating System	A program responsible for the day to day running of a computer system. Operating Systems will manage hardware, programs, memory, files and folders and will monitor computer security by maintaining accounts and permissions.	https://www.howtogeek.com/361572/what-is-an-operating-system/
OEM	Original Equipment Manufacturer – a company whose goods are used in the manufacture of another device. Your computer (for example Dell or HP) will have a CPU chip in it that is manufactured by another company (e.g., Intel or AMD). These other companies are the OEMs for your computer.	
USB	Universal Serial Bus – a common connection port used in nearly all modern computers that allows one device to connect to another. Data is transmitted serially i.e., one bit at a time along a single wire.	https://techterms.com/definition/usb



Cloud Computing	The delivery of computing services – including database servers, networking, office software and storage over the internet . To use Office 365 or Google Docs, all you need is a browser, and you can write and edit documents anywhere in the world. The file is saved on the cloud and can be accessed by anyone with the correct permissions.	https://azure.microsoft.com/en-gb/overview/what-is-cloud-computing/
Cloud Storage	This is where files or data are stored on a remote networked server, accessed using an HTTPS internet connection and are available to a user from any device and from anywhere in the world.	https://www.pcmag.com/picks/the-best-cloud-storage-and-file-sharing-services
Internet of Things	This is the concept of connecting all devices to the internet . This means that these devices can be controlled by any internet enabled device such as a laptop or smartphone and the IoT devices can send responses back via HTTP . IoT devices include Fridges, kettles, doorbells and heating systems.	https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/?sh=9426ace1d091
Attack Vector	The actual method by which an attack is delivered e.g., an infected USB stick, or phishing email.	https://www.fortinet.com/resources/cyberglossary/attack-vector
Wi-Fi	A network communication method where data is transmitted wirelessly instead of using traditional cabling methods. Wi-Fi Uses the 802.11 protocol standards.	http://www.bbc.co.uk/webwise/guides/about-wifi
Bluetooth	A network communication method where data is transmitted wirelessly instead of using traditional cabling methods. Unlike Wi-Fi, Bluetooth works only over very short ranges and required direct pairing between devices.	https://techterms.com/definition/bluetooth

All text copyright © TheComputingTutor 2020. All rights Reserved.



Vulnerability

A point of weakness in the defences of a [network](#) or System. Attackers will exploit a vulnerability to try and gain access to a system.

<https://www.upguard.com/blog/vulnerability>



Learning Aim A – Legal Responsibilities

Key term	Definition	References
Data Protection Act 1998	<p>An Act designed to make sure that Organisations take appropriate actions to safeguard people's data and information when it is stored on their systems. It has 8 principles. The key parts are</p> <ul style="list-style-type: none"> • Personal data must be adequate, relevant and not excessive • Personal data must be accurate and up to date • Personal data must not be kept for longer than is necessary • Personal data must be held securely • Personal data must be obtained for specified and lawful purposes 	<p>https://www.bbc.co.uk/bitesize/guides/zhx26yc/revision/6</p>
Computer Misuse Act 1990	<p>An act designed to make the access to a computer system or using a computer system to access other systems a criminal offence. The Act has three main principles:</p> <ul style="list-style-type: none"> • accessing computer material without permission, e.g., looking at someone else's files • accessing computer material without permission with intent to commit further criminal offences, e.g. hacking into a school computer and wanting to view your grades • altering computer data without permission, e.g., hacking into a school computer and changing your grades 	<p>https://www.bbc.co.uk/bitesize/guides/zt8qtf/revision/2</p>



Health and Safety at Work Act

An Act designed to make sure that people are kept safe in the workplace. The act can apply to general safety (making sure cables on the ground are under a mat so they cannot be tripped over) to eyesight safety (if working with monitors, staff need to be given regular breaks, regular eye tests and the brightness of the office environment needs checking).

<https://www.hse.gov.uk/legislation/hswa.htm>
<https://www.hse.gov.uk/msd/dse/>



Learning Aim A – Physical Security Measures

Key term	Definition	Resources
Physical Security	A type of security that prevents real world damage to computer systems and people, for example theft, breaking of property and environmental conditions such as fire or flood.	https://www.csoonline.com/article/3324614/what-is-physical-security-how-to-keep-your-facilities-and-devices-safe-from-on-site-attackers.html
Biometrics	A type of security system that uses a piece of biological information about a person (such as fingerprint or retina scan). Biometric data is usually highly secure as the data is usually unique to that individual and very difficult to duplicate	https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics
CCTV	Closed Circuit Television – a system whereby a set of cameras is installed on an organisations premises and can only be recorded and viewed within that premises or remotely by individuals belonging to that organisation. It is not viewable by members of the public.	https://www.paessler.com/support/it-knowledge/it-explained/cctv
On Site Data Storage	This is where your Organisations data is stored somewhere within the building or buildings that or organisation is based in.	https://www.backupassist.com/education/articles/difference-between-onsite-and-offsite-data-backup.html



Off Site Data Storage	This is where your Organisations data is stored in a different building or buildings to the one where the organisation is based in. Offsite Data Storage can also mean Cloud storage.	https://www.backupassist.com/education/articles/difference-between-onsite-and-offsite-data-backup.html
<u>Cloud Storage</u>	This is where files or data are stored on a remote networked server, accessed using an HTTPPS internet connection and are available to a user from any device and from anywhere in the world.	https://www.pcmag.com/picks/the-best-cloud-storage-and-file-sharing-services
Backups	A copy of the daily data generated by an organisation. Backups are used to recover lost or damaged data in the case of an attack. Backups are usually made at least twice a day and are normally stored Off Site somewhere. If backups are stored on-site, there is a risk of losing all an organisations data if the building is destroyed by fire.	https://www.welivesecurity.com/2019/05/10/types-backup-mistakes-avoid/



Learning Aim A – Software and Hardware security

Key term	Definition	Resources
Antivirus Software	A program that is designed to identify if a virus has infected a computer and take appropriate action. Antivirus software should be always running on a computer, constantly checking for infections. An Antivirus Program requires the use of an up-to-date Virus Definition Database to be effective.	https://www.verizon.com/info/definitions/antivirus/
Virus Definition Database	A database of all currently known viruses and what they look like (their signatures). As new viruses are released (Zero Day Viruses) eventually they will be recorded in the Database. A database needs to be downloaded to the antivirus program on a computer, so that the program is looking for all current Viruses. If a database has not been downloaded, even if an Antivirus program is running, the system is still vulnerable to attack by the latest Viruses .	https://encyclopedia.kaspersky.com/glossary/antivirus-databases/
Virus Signature	The Virus data that is stored in the Virus Definition Database. It is a sequence of binary data (1's and 0's) that identify a specific Virus .	https://www.kaspersky.co.uk/blog/signature-virus-disinfection/7799/
Heuristic techniques	A technique used by Antivirus programs where the software will scan the files that are likely to be infected with a virus . Heuristic techniques are faster than full system scans, but because they work on probability, some infected files may escape detection.	https://www.forcepoint.com/cyber-edu/heuristic-analysis



Quarantine	This is where an infected file or program is moved into a reserved, secured area of a computer system where it cannot escape and do further damage. The infected item is held here until the Security Team decides what to do with it.	https://www.safetydetectives.com/blog/how-does-antivirus-quarantine-work/
Packets	The means by which data is transmitted around networks. A packet of data contains the IP address of the sending computer (Source IP), the IP address where the packet is going to (Destination IP) the MAC address of the last computer to read the packet, and the Data (the Payload). A packet also contains header and footer information including Parity information and Packet number.	https://www.techopedia.com/definition/6751/data-packet
Packet Filtering	This is where a Firewall or Router is set up to allow only selected packets of data with known IP addresses into and out of the network .	https://www.techopedia.com/definition/4038/packet-filtering
Packet Inspection	This is where the contents of the packet of data (the payload) is examined to check for any malicious content e.g., a virus. Packet inspection will only work if the Payload Data is not encrypted (in other words is easily readable)	https://www.techopedia.com/definition/24973/deep-packet-inspection-dpi
Application Layer	The top layer of the TCP/IP stack, containing the programs and protocols for network communication such as Web Browsing (using HTTP or HTTPS), sending emails (using SMTP), receiving emails (using POP3) and transferring files (using FTP)	https://www.tutorialspoint.com/The-Application-Layer-in-TCP-IP-Model
HTTP	Hyper Text Transfer Protocol – a set of rules that determine the communication between a web browser, which sends an HTTP_REQUEST, and a reply from a web server, which sends an HTTP_RESPONSE	https://whatis.techtarget.com/definition/HTTP-Hypertext-Transfer-Protocol



FTP	File Transfer Protocol – a set of rules that allows one computer (the FTP client) to send a file to another computer (an FTP server) over the internet . The FTP client can also copy, move, delete and rename files on the server.	https://techterms.com/definition/ftp
SMTP	Simple Mail Transfer Protocol – a set of rules that allows one computer to compose and send an email. SMTP allows a device to compose a message, add attachments, define who the email is to, select CC and BCC from a list of recipients.	https://pc.net/glossary/definition/smtp
POP3	Post Office Protocol 3 – a set of rules that allows a device to download and read an email message. POP3 allows a client to read a message, delete a message, leave messages on a server, download everything to a device, mark as read and flag.	https://techterms.com/definition/pop3
<u>Firewall – Inbound</u>	The rules on a Firewall that determines what packets can come through the Firewall into the organisations network . For example, you might want to stop certain IP addresses , or IP address ranges from coming through the network to your webserver, as a form of DDOS attack. The inbound rules will stop this happening before it gets to your server.	https://searchsecurity.techtarget.com/answer/Comparing-firewalls-Differences-between-an-inbound-outbound-firewall
<u>Firewall – Outbound</u>	The rules on a Firewall that determines what packets can come through the Firewall going out of an organisations network . For example, you might know of certain IP addresses that contain malicious websites and you would want to stop an employee accidentally being taken to one of those sites by falling victim to a phishing attack.	https://searchsecurity.techtarget.com/answer/Comparing-firewalls-Differences-between-an-inbound-outbound-firewall



Learning Aim A – Software and Hardware security

Key term	Definition	References
Network Address	This is a number assigned to any device on a network to tell each device apart. Network Addresses are usually IP addresses made up of a NetID part (the ID of the network) and a HostID part (the ID of the device).	https://www.techopedia.com/definition/20969/network-address
Authentication	The process of identifying whether a user trying to access a computer, system or network is in fact that person. It is a verification process, basically checking that you are who you say you are	https://techterms.com/definition/authentication
Authorisation	The process of determining exactly what a user can do within a computer, system or network once they have been authenticated. It is basically asking “what can you do”. Authorisation involves giving permissions to Users or Groups of Users defining what they can do within the system.	https://www.techopedia.com/definition/10237/authorization
Strong Passwords	Passwords that are difficult to guess or break by brute force cryptographic techniques. They will usually contain a mixture of upper and lower case characters, numbers and special characters.	https://blog.avast.com/strong-password-ideas
Login Procedures	The process of logging into a system. The submitted login information (usually a username and password) must match that stored in the system. If it does not, then the login will fail.	
Graphical Passwords	This is where a user is required to select some specific images from a group of images. This attempts to prevent passwords being guessed by a	https://searchsecurity.techtarget.com/definition/graphical-password#:~:text=A%20graphical%20passw



	brute force attack as only the correct combination of images (e.g., select all the images that has a car) will work.	ord%20is%20an,graphical%20user%20authentication%20(GUA).
<u>Biometric Authentication</u>	This is when a user's <u>Biometric</u> Data (e.g., fingerprint or retina) is used to log into a system.	
Two step verification	This is where a second layer of authentication is required after a username or password. This could be answering a security question, picking letters from a secure word or entering a code that has just been texted to you.	https://authy.com/what-is-2fa/
Security Token – USB	This is where you have encrypted information on a target computer or system. The data can only be accessed by plugging a <u>USB</u> device that contains the decryption key to allow you access the information that you want. You have to plug the device into the computer in order for this to work.	https://www.reviewgeek.com/63448/what-is-a-usb-security-key-and-should-you-use-one/
Security Token – Near Field	This is where a security 'token' (a piece of code that identifies a user) is included on a card or a device (like a phone for Apple Pay). A device with Near Field Communication enabled will detect the presence of the card / device when it comes within range (e.g., if the card is tapped onto the NFC device) and will use the token information to log the user into the system with the correct authorisation levels.	https://squareup.com/gb/en/townsquare/nfc
Knowledge Based Authentication	This is where you have to answer a series of questions in order to be authenticated e.g., 'what's the name of your first pet'. The questions and answers are unique to you. The idea is that security is based around knowledge that is unique to the individual, rather than a guessable password.	https://searchsecurity.techtarget.com/definition/knowledge-based-authentication



Kerberos Authentication

This is a process using symmetric key cryptography (the same key is used to encrypt and decrypt a message) and a third-party verifier. The idea is that a user is given an encrypted 'ticket' for use while they are logged in. The idea is that this encrypted ticket will allow a user to access all services in a system without a user having to send their login details over the [internet](https://www.bmc.com/blogs/kerberos-authentication-what-is-it-how-it-works/).

<https://www.bmc.com/blogs/kerberos-authentication-what-is-it-how-it-works/>



Learning Aim A – Software and Hardware security

Key term	Definition	References
<u>Access Control</u>	A set of rules that determines what a user can do on a piece of data within a system. Permissions include read, write and execute. Access control can be thought of as permissions that have been actually applied to a piece of data saying who can do what.	https://www.csoonline.com/article/3251714/what-is-access-control-a-key-component-of-data-security.html
Trusted Computing	'Trusted computing' (TC) is the idea that all new hardware and software technologies will have ready-made, built-in processes to deal with and fix any basic security problems and user challenges that may occur. All new hardware is required to stop programs from accessing each others memory, deal with spyware and securely store any encryption keys.	https://searchsecurity.techtarget.com/definition/trusted-computing
Encryption	The process of turning a readable message (the plain text) into an unreadable message (the cypher text) using a rule or algorithm (the cypher key). Making a message unreadable is called Encryption and turning the message back into its readable form is Decryption.	https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences
Symmetric Encryption	In symmetric encryption the same key is required to encrypt and decrypt the message	https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences



Asymmetric Encryption	Here, a public key is required to encrypt the message and a different private key is required to decrypt the message. It is not possible to decrypt the message without the Private Key. This is the basis of HTTPS communication using RSA and SHA-1 encryption.	https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences
DRM	Digital Rights Management is a way to protect copyright of downloadable digital material. For example, it prevents users being able to make copies of the material or installing it on more than one device. If the material has been purchased as part of a subscription, DRM can make the material unavailable after a certain period of time. DRM requires that the documents be connected to a DRM server that manages how the material is used.	https://digitalguardian.com/blog/what-digital-rights-management
Onion Router (TOR)	This is an open-source program that allows users to protect their privacy and security against Internet Surveillance. Using TOR is sometimes referred to as 'The Dark Web' since everything is hidden from view.	https://whatis.techtarget.com/definition/TOR-third-generation-onion-routing
VPN	Virtual Private Network – this is a secure tunnel through the internet where all traffic is encrypted. It is used for people working remotely who want full secure access to a company network . A VPN server maintains a trusted list of IP addresses . The remote worker will connect to the VPN server using a trusted IP address and then all communication from then on is encrypted.	https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html
Digital Certificate	A small file issued to a website provider that proves that they are who they say they are. When you connect to a website, your browser will request the sites digital certificate, and if valid you know that you are	https://www.techslang.com/definition/what-is-a-digital-certificate/



	going onto a trusted site. Digital Certificates are issued by a Certificate Authority.	
Certificate Authority	A company whose job it is to visit and investigate all organisations that have a website to make sure that they are who they say they are. A certificate Authority would visit an organisations premises and ask to see all bank records and organisational data. Once the Certificate Authority is happy that the organisation is legitimate, a digital certificate is issued. An example of a Certificate Authority is Verisign.	https://www.thesslstore.com/blog/what-is-a-certificate-authority-ca-and-what-do-they-do/
<u>HTTPS</u>	Hyper Text Transfer Protocol (Secured) - A version of HTTP where the communication between the browser and the website is encrypted using SSL (Secure Sockets Layer). SSL will encrypt the data with either RSA or SHA-1 encryption algorithms. This is used for submitting sensitive data over the internet , such as bank details or passwords.	https://techterms.com/definition/https
MAC Address	Medium Access Control Address – a 48-bit HEX code address that is burned onto each Network Interface Card on a device. A device might have a single IP address but multiple MAC addresses if they have multiple NIC's. Each MAC address is globally unique – i.e., there are no two network cards on the planet with the same MAC address.	https://whatismyipaddress.com/mac-address
MAC Filtering	This is when a router is configured to only allow devices with a specific MAC address to connect to the network . Even if a device has a valid IP address and the correct Wi-Fi password, if the device MAC address is not in the list of trusted devices, the new device cannot connect to the network. It is a way of restricting use of a network to a specific number of known devices with known MAC addresses.	https://www.lifewire.com/enabling-mac-address-filtering-wireless-router-816571



SSID	Service Set Identifier – another name for the name given to your Wi-Fi network. This means that if you have a list of available Wi-Fi network, each will have its own SSID and you will know which one you need to join. It also makes sure that packets of data are transmitted to the correct network .	https://techterms.com/definition/ssid
WEP	Wired Equivalency Protocol – a protocol designed to try and give wireless networks the same level of security as a wired network. This requires logging in to the network with a username and password and then all data is encrypted from then on using 128 bit encryption. WEP was widely cracked in early 2000 and was officially retired in 2004. This should not be used.	https://www.howtogeek.com/167783/htg-explains-the-difference-between-wep-wpa-and-wpa2-wireless-encryption-and-why-it-matters/
WPA2	Wi-Fi Protected Access is an improvement over WEP as it uses 256 Bit encryption. It also checks to see if any packets had been tampered with.	https://www.howtogeek.com/167783/htg-explains-the-difference-between-wep-wpa-and-wpa2-wireless-encryption-and-why-it-matters/
WPS	Wi-Fi Protected Setup is used for setting up wireless networks in the home. It allows a new wireless device to 'pair' with the existing Wi-Fi Router once the WPS buttons on both devices have been pressed. This will only work if the router is set to use WPA2. It will not work with WEP.	https://www.technipages.com/what-is-wps



Learning Aim B – Network Types

Key term	Definition	Resources
Network	This is where two or more devices are connected together, so that they can communicate with each other and share files and data.	https://techterms.com/definition/network
LAN	Local Area Network – a network (which is either wired or wireless) that is over a small area such as a home, a floor in a building or between buildings.	https://www.cisco.com/c/en/us/products/switches/what-is-a-lan-local-area-network.html
WLAN	Wireless LAN – A local Area Network that is composed of one or more purely wireless networks.	https://searchnetworking.techtarget.com/answer/Wireless-vs-Wi-Fi-What-is-the-difference-between-Wi-Fi-and-WLAN
WAN	Wide Area Network - a network (which is either wired or wireless) that is over a large geographic area – such as between cities or between countries.	https://www.comptia.org/content/guides/what-is-a-wide-area-network
SAN	Storage Area Network – a network that contains multiple dedicated storage devices available for use by other computers or networks. SAN typically use Fibreoptic cables to deal with the amount of data that will be read from or written to the storage devices on the network. SAN networks appear like extra hard drives to a computer.	https://techterms.com/definition/san



PAN	Personal Area Network – a wireless network that operates over a very short distance, about 5 metres. This is usually another name for a Bluetooth network	https://www.nibusinessinfo.co.uk/content/personal-area-networks
Intranet	A network , usually web based, that belongs to an organisation and is only available to members of that organisation from within the organisation's building. To use an intranet, you need to be physically sat at, and logged into, a computer within the building.	https://socialchorus.com/blog/what-is-an-intranet-and-is-it-still-relevant-to-your-organization/
Extranet	A network , usually web based, that belongs to an organisation and is only available to any authorised members of that organisation if they are logged into the network, even remotely. If you want to use an extranet remotely you usually need to be logged in using a VPN . These have now been replaced by cloud computing and storage .	https://socialchorus.com/blog/what-is-an-intranet-and-is-it-still-relevant-to-your-organization/
Internet	A network of networks spread across the globe. Each device on the internet needs an IP address to be discovered. The networks are joined by global routers. This is not the same as the World Wide Web. Communication mostly happens using TCP/IP .	https://socialchorus.com/blog/what-is-an-intranet-and-is-it-still-relevant-to-your-organization/
Cloud	The idea of putting programs or storing files and folders on a device connected to the internet . These programs or data can be connected to from any device anywhere on the planet if the correct usernames and passwords are supplied. Being able to use programs on the cloud is called Cloud Computing . Being able to store files and folders on the Cloud is called Cloud Storage .	https://www.cloudflare.com/en-gb/learning/cloud/what-is-the-cloud/



Physical Topology	The way in which network cables are actually laid out in the real world to connect computers together. A topology can be considered a map that plots the available routes for packets of data.	https://www.geeksforgeeks.org/difference-between-physical-and-logical-topology/
Star Topology.	A topology where there is a central device node (router / switch / hub) and each networked device is connected to this. The idea is that a packet of data is transmitted to the central node and the packet is then directed to the correct destination. If the central node fails, the entire network fails.	https://www.bbc.co.uk/bitesize/guides/z36nb9q/revision/6
Extended Star	This is where several star networks are joined together by a single central node. This means that if this central node fails, the entire network fails, however it is possible for individual star networks to fail but the rest of the network will function. This is called multiple points of failure. The extended star is used in larger business networks.	https://www.itprc.com/a-guide-to-network-topology/
Wireless Mesh	This is a network that uses many wireless nodes that shares a single network connection to provide a wide area wireless coverage. Wireless Mesh networks only has a single node that needs to be connected to the Internet . It's like putting in Wi-Fi range extenders in your home that will allow any device to connect to the Internet anywhere without any loss in signal.	https://computer.howstuffworks.com/how-wireless-mesh-networks-work.htm
BYOD	Bring Your Own Device – was a strategy adopted by organisations as a way of saving money on buying new hardware for employees. The idea was that you brought your own personal device (phone or computer) and connected to the company network. The idea showed serious issues of network security risks and device compatibility problems.	https://www.techradar.com/uk/news/computing/what-is-byod-and-why-is-it-important-1175088



Logical Topology	This is the idea of what the network is going to look like. In a logical topology you would define how the devices are connected and what hardware and cables you would need and then how they would communicate with each other. When you come to actually put the cables and devices into your building, you are turning the logical topology into the physical topology.	https://www.educba.com/logical-topology/
Ethernet	A network topology where all devices share a single wire. A packet of data is sent down the wire and inspected by each computer on the Ethernet. When the packet reaches the computer with the matching destination IP address , the packet is received by that computer.	https://searchnetworking.techtarget.com/definition/Ethernet
Wireless (802)	A set of protocols that allow packets of data to be sent using radio transmission to devices belonging to the same SSID . The first protocol was 802.11a, followed by 802.11b, 802.11g, 802.11n and currently 802.11ah. The issue is backwards compatibility – an 802.11a router cannot use a 802.11ah protocol.	https://www.networkworld.com/article/3238664/80211x-wi-fi-standards-and-speeds-explained.html
Peer to Peer	This is where two or more computers are directly connected to each other to share files or services. If you want to add a new user account, you need to add it to each machine on the network manually. If you want to add a new device, you need to manually configure it, so it has all the same data as each other device on the network.	https://www.computerworld.com/article/2588287/networking-peer-to-peer-network.html
Client	A device that requests the services provided by a server on a network. It you send a file to a printer, you are acting as a client.	https://isaacomputerscience.org/concepts/net_network_client_server_p2p



Server	A device on a network that provides a specific set of services to a client and will notify the client when such services have been provided. A print server will allow printing services such as: print all pages, print colour, print greyscale. The messages that come back from the print server include: printing complete, out of paper, out of toner.	https://isaacomputerscience.org/concepts/net_network_client_server_p2p
Client/ Server	A client server network is when network requests (such as login details and device IP addresses) are managed by a network server and each client device will request these services each time a user wishes to connect to a network.	https://www.omnisci.com/technical-glossary/client-server
Thin client	The idea of a computer having only browser software installed and every other piece of software is installed on a cloud server. The software is delivered down the internet and run from within the browser. Office 365 is designed for a thin client: Word, Excel and PowerPoint are never installed on the client device but are run from within a browser.	https://www.fortinet.com/resources/cyber-glossary/thin-client
Virtualisation	The process of turning a physical IT Infrastructure (servers, cables, installed programs) into a software alternative, usually delivered over the internet . Virtualisation of a network usually involves Cloud Computing and Cloud Storage as programs and data are moved away from hardware in an organisation's premises and onto a Cloud Server.	https://www.itpro.co.uk/612016/what-is-virtualisation



Learning Aim B – Network Components

Key term	Definition	References
Device	Any device that is connected to a network . This could include a computer, printer, scanner, mobile phone, switch or router	
Switches	A networking device that usually serves as the central node of a star network and maintains a list of all connected devices. When one device wants to send a packet of data to another device, the switch examines the destination IP address of the packet and transmits the packet to that computer. Switches can only connect devices together.	https://techterms.com/definition/switch
Routers	A networking device that usually serves as the central node of an extended star network and maintains a list of all connected devices and networks. When one device wants to send a packet of data to another device, the switch examines the destination IP address of the packet and transmits the packet to that computer or network. Routers can connect devices and networks together.	https://www.cisco.com/c/en_uk/solutions/small-business/resource-center/networking/what-is-a-router.html
Hub	A networking device that usually serves as the central node of a star network. When one device wants to send a packet of data to another device, the hub transmits the packet all devices connected to it. Hubs can only connect devices together.	https://www.computerhope.com/jargon/h/hub.htm



Wireless Access Points	Devices used to allow wireless devices access to a wired network . A Wireless Access Point will be wired into a physical network and will provide connectivity to wireless devices within a short distance of the access point. The more wireless access points in an organisation, the better the wireless coverage.	https://www.lifewire.com/wireless-access-point-816545
MFD	Devices that can perform multiple functions. Typical MFD devices are machines that can Print, Copy and Scan.	https://www.simple.scot/what-is-a-multi-functional-device/
Modem	A device that converts computer data from one network transmission type (your phone line, fibreoptic cable) and convert it to another transmission type (WiFi or Ethernet). Most home routers have modems built in to them.	https://www.linksys.com/us/r/resource-center/what-is-a-modem/
Cables	The wires that are used to connect devices together. Cables could be Co-Axial, Fibreoptic, Serial, Parallel or Ethernet.	
Fibreoptic	A means of data transmission that uses flashes of light to represent binary 1's and 0's. Fibreoptic cable is the fastest transmission medium and is very secure, however it is expensive and very fragile.	https://www.verizon.com/info/definitions/fiber-optics/
Wireless	The process of transmitting data using radio frequencies. Typical frequencies in the home are the 2.4GHz and 5GHz frequencies. This is the transmission medium for WiFi networks.	https://www.cisco.com/c/en_uk/solutions/small-business/resource-center/networking/wireless-network.html



Flash Drives	A flash drive is a small, portable storage device that, unlike typical magnetic storage devices, has no moving parts. Flash drives are therefore very quiet, very fast and consume less power than traditional hard disk drives. However, they typically store less data, are more expensive and when the drive eventually fails, no data can be recovered from it.	https://www.lifewire.com/what-is-a-flash-drive-2625794
Optical Media	A device used to store data on read/ write physical media such as CD's, DVD's or Blu Rays. Data needs to be physically burned onto the surface of the media using a laser. Data is read by measuring the difference in light from a laser being reflected from the disk surface. Optical media as a storage device is rarely used any more, replaced in favour of flash drives or Cloud Storage .	https://techterms.com/definition/optical-media
Network OS	An operating system installed on a server that is responsible for not only running and managing that server but also managing the network of devices connected to it. The network OS will typically contain a network directory service and manage Authentication and Authorisation .	https://www.tutorialspoint.com/network-operating-system-rtos
Device OS	An Operating System that is installed on a device, typically a computer or server, responsible for running and managing only that device.	https://techterms.com/definition/operating-system



Performance Monitor	A software application that allows a user to view the current performance of a network . Performance monitor will show how much of the network is being used, what devices are connected and how much data is being transmitted by each device. A performance monitor will usually allow an administrator to identify any device that is causing the network to run slowly.	https://www.riverbed.com/gb/faq/what-is-network-performance-monitoring.html
Event Viewer	An event monitor will allow an administrator to view any network events that have happened. Network events could be e.g., successful log-ins, failed log-ins, connection failures, router or switch failures. The event viewer is one of the key tools in security forensics as this will give a picture of what was going on in the network	http://what-when-how.com/networking/event-monitoring-and-reporting-networking/
Log Viewer	Network events will usually be recorded in a log. Log viewers allow administrators to view a list of events to see what happened in the event of a network incident.	https://www.solarwinds.com/log-analyzer
Vulnerability Scanners	These are automated software tools that can scan a network for vulnerabilities . Scanners could include checking to see if any Firewall Ports have been left open or to see if any computers on the network do not have the latest, up to date Virus Definition Database .	https://www.redlegg.com/blog/what-is-vulnerability-scanning-and-how-does-it-work
Packet Sniffers	Intrusion software that scans packets of data on a network and attempts to read the Payload of data. If the data is not encrypted, the contents of the packet can be read.	https://www.kaspersky.com/resource-center/definitions/what-is-a-packet-sniffer



Networked Database Server

A [server](#) that provides database services across a [network](#). A [client](#) will be able to connect to the database and perform SELECT, UPDATE, INSERT and DELETE commands. The [server](#) will confirm that the connecting [client](#) has the correct [authorisation](#) permissions to perform the requests.

<https://ecomputernotes.com/fundamental/what-is-a-database/what-is-a-database-server>

Networked File Server

A [server](#) that provides file services across a [network](#). A [client](#) will be able to connect to the file server and perform file commands such as OPEN, CLOSE, COPY, MOVE, DELETE and RENAME. The [server](#) will confirm that the connecting [client](#) has the correct [authorisation](#) permissions to perform the requests.

https://techterms.com/definition/file_server



Learning Aim B – Network Services and Resources

Key term	Definition	Resources
TCP/IP	Transmission Control Protocol over Internet Protocol. A set of rules for how packets of data move around the <u>internet</u> . TCP/IP has four layers: Application, Transport, Network and Link. The protocol involves splitting a message into packets of data and adding source and destination IP addresses. At the receiving computer the Transport Layer will check to see if all <u>packets</u> have arrived and are not damaged, and if they are it will request the missing or damaged packets be resent. TCP/IP is a means to guaranteeing that the message will be delivered.	https://www.avast.com/c-what-is-tcp-ip
Ports	A number corresponding to the start and end point of a communication. Web based communication using <u>HTTP</u> uses Port 80. Ports correspond to cable sockets in <u>Firewall</u> where that specific traffic is allowed to pass through.	https://www.cloudflare.com/en-gb/learning/network-layer/what-is-a-computer-port/
IP v4 Addresses	An IP address defines all public routable devices on the <u>internet</u> as well as private devices on networks. IPv4 was a 24-bit sequence of numbers in four groups of 8 bits going from 0 – 255 e.g. 34.185.92.113. We ran out of IPv4 addresses in 2011. IP Addresses are made up of NetID's (the ID of the Network) and HostID's (the ID of the Device)	https://www.uptrends.com/what-is/ipv4



IP v6 Addresses	IP v6 is a 128-bit number sequence that allows for more internet enabled devices. IPv6 also allows for larger data payloads than IPv4.	https://whatismyipaddress.com/ip-v6
Private Addresses	All corporate and home network devices are allocated private IP addresses. These IP addresses are not visible to devices on the internet but allows all devices on the network to communicate with each other. Typical private IP addresses have a NetID of 192.168.	https://www.tutorialspoint.com/difference-between-private-and-public-ip-addresses
NAT	Network Address Translation – if a device on a private network communicates with a computer with a public IP address, there needs to be a way for the network router to know which private device on the network was using this service. NAT is the process of converting a private IP address into a Public IP address.	https://whatismyipaddress.com/nat
Domain	Another name for a network of devices.	https://techterms.com/definition/domain
SubDomain	A name given to part of a network domain. A Domain can contain one or more sub domains. There might be a sub domain for a floor in a building, or for a group of employees.	
Network Segmentation	The process of splitting a network into multiple SubDomains. Each network segment will have its own NetID part of the IP address . The network administrator can decide what traffic can move between segments.	https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html



DNS	Domain Name Service – the process of converting a human readable website address (e.g. www.bbc.co.uk) into an IP address (212.58.237.253)	https://www.cloudflare.com/en-gb/learning/dns/what-is-dns/
Directory Services	A list of all entities on a network , with information about each entity. For example, devices would have IP addresses and device type (computer, printer, server, etc.). Users would have their authentication and authorisation details stored here. Directory services are used by Network Operating Systems to manage the running of the network . Common directory services are Active Directory (on windows networks) and LDAP (on Unix Networks)	https://www.dummies.com/programming/networking/defining-terms-what-is-a-directory-service/
DHCP	Dynamic Host Configuration Protocol – a service provided by a router or directory that allocated each device on the network with a unique IP address for that network. If DHCP is disabled, then IP addresses need to be manually added to each device and these are usually static (will not change). If a device disconnects and reconnects to a network, it will be given a new IP address by DHCP.	https://searchnetworking.techtarget.com/definition/DHCP
Routing	The process of moving packets of data from one network to another network based on the packet destination IP address . Routers use Routing Tables to identify the path that a packet of data needs to take to get to its destination.	https://www.cloudflare.com/en-gb/learning/network-layer/what-is-routing/



Remote Access Services

Services provided by an organisation that allow employees to access the network remotely from home or while on the move. This could include the ability to log into their computer from home or to access company files or data. This has been replaced by [Cloud Storage](#) and [Cloud Computing](#). Remote access usually uses a [VPN](#).

<https://www.dnsstuff.com/what-is-remote-access-definition>



Learning Aim B – Network Services and Resources

Key term	Definition	Reference
File Service	A server that provides file services across a network . A client will be able to connect to the file server and perform file commands such as OPEN, CLOSE, COPY, MOVE, DELETE and RENAME. The server will confirm that the connecting client has the correct authorisation permissions to perform the requests.	https://en.wikipedia.org/wiki/File_server
Print Service	A server that provides printing services across a network . A client will be able to connect to the print server and perform print commands such as PRINT, PRINTALL, PRINT SELECTED, PRINT COLOUR. The server will confirm that the connecting client has the correct authorisation permissions to perform the requests.	https://www.printerland.co.uk/blog/how-does-a-print-server-work/
Web Service	A server that allows a web client to connect to the server and perform HTTP_REQUEST commands such as GET and POST. The server will confirm that the connecting client has the correct authorisation permissions to perform the requests and issue an HTTP_RESPONSE.	



Mail Service

A [server](#) that provides email services across a [network](#). A [client](#) will be able to connect to the email server and perform email commands such as SEND, REPLY, REPLY ALL, CC, BCC etc. The [server](#) will confirm that the connecting [client](#) has the correct [authorisation](#) permissions to perform the requests.

<https://www.samlogic.net/articles/mail-server.htm>

Communication Service

A [server](#) that provides communication services across a [network](#). A [client](#) will be able to connect to the server and request for communication to be carried out using video or audio. The [server](#) will confirm that the connecting [client](#) has the correct [authorisation](#) permissions to perform the requests. Examples of communication servers are Teams, Zoom and Skype.

<https://smallbusiness.chron.com/use-networkbased-communications-tools-business-59382.html>



Learning Aim C – Vulnerabilities

Key term	Definition	Reference
Penetration Testing	The process to test a network defences for vulnerabilities . The purpose of the penetration test is to firstly see if the network can be breached, and then to see exactly how far into a network an attacker can get and what information is visible to the attacker. After a penetration test, it should be possible to fix the flaws in the network defences.	https://www.ncsc.gov.uk/guidance/penetration-testing
Risk	A threat that could result in some loss at some point in time.	
Risk Severity	The probability of the threat occurring multiplied by the level of damage that the threat will do.	
Probability	How likely it is that a threat will occur. Probability is either Very Likely, Likely or Unlikely. 10 years ago, it was Unlikely that a school or college would be targeted for a ransomware attack. In 2020, schools and hospitals are Very Likely targets for a ransomware attack.	
Impact Level	What would the impact be on an organisation if the data loss happened? There are three categories: Minor, Moderate and Major.	



Risk Severity Matrix

A grid that plots the probability of a threat occurring against the amount of damage the threat will inflict on an organisation. The most extremes are a Very Likely threat causing major damage (this is an Extreme Severity Threat) to an Unlikely threat causing minor damage (this is a Low Severity Threat)



Learning Aim D – Documentation

Key term	Definition	References
Policy	A set of rules that an employee in an organisation is expected to follow.	
Internet Policy	A set of rules that says what an employee can or cannot do while using the internet during working hours and while using an organisations equipment.	https://www.lawdonut.co.uk/business/employment-law/employment-policies/an-internet-policy-for-your-employees
Email Use Policy	A set of rules that says what an employee can or cannot do using an organisations email during working hours and while using an organisations equipment.	https://whatis.techtarget.com/definition/corporate-email-policy
Security Policy	A set of rules that says how an organisation is expected to maintain security of an organisations data or equipment. Security policies will also list the expectations of its employees in helping to keep data secure e.g. not giving out passwords, or taking home unencrypted data.	https://www.paloaltonetworks.com/cyberpedia/what-is-an-it-security-policy
Password Policy	A set of rules that says how an organisation is going to manage its passwords and password security.	https://blog.devolutions.net/2018/02/top-10-password-policies-and-best-practices-for-system-administrators



Security Audit	A process by which the current security state of each device in a network is assessed. A security audit would show if each device is up-to-date with e.g. OS updates, Virus Scans, Virus Database Definitions. An Audit will also review existing security policies to make sure that they are up to date with current legislation and to make sure that they are being carried out by the organisation effectively.	https://www.nexor.com/what-is-a-security-audit/
Backup Policy	A set of rules that says how an organisation is going to back up it's data. A Backup policy will specify what data is being backed up, where it is being backed up to and how often a backup will take place.	https://clouddolphin.co.uk/the-importance-of-data-backup-policies/
Data Protection Policy	A set of rules that says how an employee is going to ensure it complies with all principles of the Data Protection Act.	https://www.techopedia.com/definition/30183/data-protection-policy
Incident response Policy	The steps that an organisation should follow in the event of a Cyber Security Incident.	https://www.ncsc.gov.uk/collection/incident-management/cyber-incident-response-processes
CSIRT	Cyber Security Incident Response Team – the people responsible for implementing the Incident Response Policy after a Cyber Security Incident. There would normally be a Team Leader and one or more technical experts including an Incident Lead.	https://www.ncsc.gov.uk/collection/incident-management/creating-incident-response-team



Disaster Recovery Policy	The steps that an organisation should follow to recover any lost or damaged data in the event of a Cyber Security Incident. This should at least involve recovering lost data from backups.	https://www.ibm.com/services/business-continuity/disaster-recovery-plan
External Service Provider	An External Service Provider is a company or organisation that provides services to other organisations. These services could be backup services, cloud storage or computing services or disaster recovery services. Other services could be hardware providers (e.g., an organisation could have a relationship with Dell computers to provide all computers, monitors and servers for that organisation)	https://en.wikipedia.org/wiki/Service_provider
Legal Ownership	This is an agreement with the External Service Provider about exactly what responsibilities the service provider has and what the organisation has. It basically says who will do what e.g., if a computer supplied by Dell goes wrong within a week, Dell should replace it. If an employee spills a drink into the computer and damages it, the organisation should replace it.	
Security Protection	This is an agreement with the External Service Provider about exactly what responsibilities the service provider has and what the organisation has regarding data security. For example, if an organisation puts all their data on an External Service cloud, and the cloud is breached, then the security agreement would need to determine who was responsible for the breach and what to do afterwards.	



Dispute Resolution

This is the process of settling a disagreement between an External Service Provider and an organisation if there has been any concerns about security or legal ownership.



Learning Aim E – Data Forensics

Key term	Definition	Resources
Forensics	The process of sifting through available evidence to find the cause of a Cyber Security Incident and to identify who was responsible and what was lost or stolen.	https://searchsecurity.techtarget.com/definition/computer-forensics
Desktop Forensics	The process of taking away a computer to study later by looking through all available logs and monitors on the computer. The computer has been isolated from a network and is no longer in use.	https://searchsecurity.techtarget.com/definition/computer-forensics
Live Forensics	The process of carrying out forensic analysis in a live business environment when computers / servers are still in use and the data is constantly changing.	https://en.wikipedia.org/wiki/Computer_forensics
<i>In Situ</i>	Latin for 'on site'. This means that any forensic analysis will be happening where the Incident took place.	
Network Forensics	The process of reviewing network security to determine the location of any network intrusion. This would involve looking at Firewall logs, server logs and running scans of the Firewall ports .	https://www.itpro.co.uk/cyber-attacks/31660/what-is-network-forensics



Snapshot

Capturing the state of a [network](#) at a particular moment in time. This is used particularly in live forensics, so that how the network and devices and devices appeared at the time of the incident can be recreated and studied at a later date.

False Positive

When you think you have found the cause of the Cyber Security Incident, but it is not actually the case.





**The
Computing
Tutor**

“Inspiring Students to Succeed”

www.thecomputingtutor.com

No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the TheComputingTutor

All text copyright © TheComputingTutor 2020. All rights Reserved.

