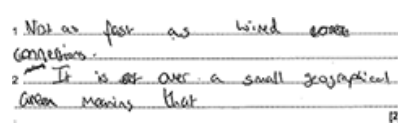




Mark scheme

Question			Answer/Indicative content	Marks	Guidance
1		i	<p>1 mark from:</p> <ul style="list-style-type: none"> • Uses dedicated/own/internal hardware / no external/third party hardware/infrastructure / computers use MAC addresses to communicate within the LAN 	1	<p><u>Examiner's Comments</u></p> <p>Candidates often gave a benefit of a LAN instead of a characteristic. This was often in comparison to a WAN. Examples included that it is cheaper, or that you can share devices and transfer data. Some responses identified the use of owner-owned hardware, or that third-part hardware was not required.</p>
		ii	<p>1 mark each to max 4: e.g.</p> <ul style="list-style-type: none"> • Allows more devices to connect ... • ...for example televisions, mobile phones • Easy to connect (devices) / Easier to setup (wireless connections) / By example e.g. easier for guests to connect their devices • Home is likely small area • ... so short distance wireless is sufficient • Devices can move around / can use devices in different areas / can connect from anywhere in the house / can use where wires don't reach / can access from a larger area (than wired) • ... by example e.g. student is using a laptop so does not need to be tied to one place / by example e.g. they don't have to disconnect before moving / e.g. they can stay connected whilst moving • Cheaper to purchase/install/setup for new devices / no cost for (new/replacement) wires/hardware 	4	<p>Easier/cheaper on their own is NE</p> <p><u>Examiner's Comments</u></p> <p>Candidates were often able to explain the benefits of including wireless connections. Common answers included the ability to be mobile and move around the home and allowing a wider range of devices to connect to the network.</p> <p>Some candidates extended their answers by explaining or justifying the wider range of devices. For example by stating mobile phones do not have wired ports.</p> <p>Some responses answered the question as though it was excluding wired connections all together and that the wires were being replaced; this did not answer the question asked which was the benefits of it</p>

		<ul style="list-style-type: none"> ...because no additional/fewer wires are needed Fewer trip hazards from trailing wires / reduce risk of damage to cables / fewer cables to damage More compatible / some devices only have wireless connections 		including wireless – as well as wired.
	iii	<p>1 mark each to max 2: e.g.</p> <ul style="list-style-type: none"> Prone to interference / by example Limited range of signal Slower rate of transmission / less bandwidth / reduced network performance/ increased latency / BOD slower connection / more users reduces rate of transmission / bandwidth /performance etc. Increased risk of security concerns / by example e.g. A hacker could connect to the wireless connection Less stable connection Higher chance of collisions / Higher error rate 	2	<p>MP3 needs to say what is slower / decreased e.g. It's slower, is NE</p> <p>Mark first drawback in each answer space.</p> <p>Less reliable is TV on its own for MP 5</p> <p><u>Examiner's Comments</u></p> <p>Candidates often demonstrated a good understanding of the drawbacks of wireless connections. Common responses included lower bandwidth and possible interference from other devices and/or objects.</p> <p>In this response some candidates stated that wireless connections could be slower – but did not give enough information to explain what was slower.</p> <p>Exemplar 1</p>  <p>The response in Exemplar 1 has identified that wireless is "not as fast as wired connections". However, the candidate has not specified what it is not as fast at doing.</p>

					To gain the mark, the candidate could refer to the transmission speed, the speed that errors are corrected, the speed that it loads, etc.																									
			Total	7																										
2	a		<p>1 mark for each row</p> <table><tr><th>Threat</th><th>Anti-malware</th><th>Penetration testing</th><th>Encryption</th><th>Firewall</th></tr><tr><td>Spyware</td><td>✓</td><td></td><td></td><td>(✓)</td></tr><tr><td>Brute-force attack</td><td></td><td>(✓)</td><td></td><td>✓</td></tr><tr><td>Data interception</td><td></td><td></td><td>✓</td><td></td></tr><tr><td>SQL injection</td><td></td><td>✓</td><td></td><td>(✓)</td></tr></table>	Threat	Anti-malware	Penetration testing	Encryption	Firewall	Spyware	✓			(✓)	Brute-force attack		(✓)		✓	Data interception			✓		SQL injection		✓		(✓)	4	<p>(✓) can be present, or not</p> <p><u>Examiner's Comments</u></p> <p>This question required candidates to consider which methods would be appropriate to prevent each threat. For each threat there was one method that was most appropriate. Some threats had other suitable responses. Some candidates did not take note of these instructions and only ticked one box for each row, commonly missing another appropriate method.</p> <p> Misconception</p> <p>A common misconception was that a firewall and penetration testing could stop data interception. Both of these methods would prevent access to a computer system, but if data is being transferred between computers (for example on the internet) then there will be no firewall to stop the interception.</p>
Threat	Anti-malware	Penetration testing	Encryption	Firewall																										
Spyware	✓			(✓)																										
Brute-force attack		(✓)		✓																										
Data interception			✓																											
SQL injection		✓		(✓)																										
	b		<p>1 mark for threat 1 mark each to max 2 for description e.g.</p> <ul style="list-style-type: none">Threat: Social engineeringUsing deception to manipulate users...to gain personal data	3	<p>If threat is clearly wrong do not FT.</p> <p>If no threat given, read description for name of threat. If no name, do not award.</p> <p>If threat is vague award matching description.</p>																									

		<ul style="list-style-type: none"> • Threat: Shoulder surfing (threat or expansion) • Watching a person entering a password • ...and using it to access an account • Threat: Phishing • Fake emails sent to person / click on link from fake email • Person sends personal data / gives away personal data • Threat: Pharming • Software that redirects user to fake website / use of a fake website • Person enters personal data / gives away personal data • Threat: Denial of service / DOS / DDOS • Multiple requests sent to a server (simultaneously) / server is flooded with requests • More requests than the server can process / uses all of the bandwidth available • Server cannot respond / server crashes/denies access / stops access to a network / slows access to a network • Threat: Hacker • Person gaining unauthorised access to a system/account • To delete/damage/access data • Threat: Virus/malware • Software that replicates/spreads • Fills disk space • Deletes/corrupts data / allows unauthorised access • Threat: Trojan • Malware disguised as legitimate software • Once installed acts as a virus / by example of action e.g. deleting files / allows unauthorised access • Threat: Worm • Software that replicates across a network • Uses up all the bandwidth • Threat: Ransomware • Encrypts/corrupts/locks access to data • Cannot access data without paying a fee/money / pay fee/money to get 	<p>Allow social engineering as the threat – naming and description of phishing/pharming/shoulder surfing in the description.</p> <p>Ransomware – MP3 cannot be awarded for 'ransom' on its own without reference to it being paid.</p> <p>For actions that the malware/virus etc. can carry out – award any feasible action.</p> <p><u>Examiner's Comments</u></p> <p>Many responses accurately identified another threat. The most common responses were denial of service or virus. Some responses gave a keylogger which was a repeat of spyware because it is a specific type of spyware.</p> <p>DDOS was often described appropriately, although some responses described it as being an attack on an individual's device instead of a server. Virus was also often described appropriately with the possible effects of deleting or corrupting files.</p> <p>Some responses described how to prevent the threat instead of describing the threat itself.</p>
--	--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

			<p>them back/decrypted / Cannot access data without meeting demands</p> <ul style="list-style-type: none"> • Threat: Physical threat / by example • Damage to hardware • Deletes/corrupts data 		
			Total	7	
3			<p>1 mark each to max 2</p> <p>e.g.</p> <ul style="list-style-type: none"> • Data cannot be understood if intercepted / The data will be meaningless • So that only authorised users can access the confidential material / protect confidential / personal / user / library data • To follow legislation/DPA 	2	<p>Question is transmission not storage</p> <p>Candidates might answer in terms of why encryption is good, or why the current system is not good. If the candidate has not clearly said which they are talking about (e.g. the current system or encryption means....) then the reverse of each mark point can be given.</p> <p><u>Examiner's Comments</u></p> <p>Some candidates were able to identify that encryption makes it impossible to understand the data.</p> <p>Some candidates stated the data could not be read. This was not precise enough. The data can still be intercepted and read but that this data will be meaningless.</p> <p>Some candidates also appropriate applied their answers to this scenario, identifying that it meant the data the library was transmitting, e.g. personal/sensitive data, could not be stolen or used inappropriately.</p> <p> Misconception</p> <p>A common misunderstanding</p>

					was that encryption stops data being intercepted. The data can still be intercepted, but when opened it will be meaningless.
			Total	2	
4	a		<p>1 mark each to max 2 e.g.</p> <ul style="list-style-type: none"> • Locks • Keycard entry • Biometric entry to room • Passcode entry to room • Alarms • Security guards/team • CCTV 	2	<p>Secure room/device is TV</p> <p>Mark first in each answer space</p> <p>Do not award password, but do award passcodes/word on doors.</p> <p><u>Examiner's Comments</u></p> <p>Some candidates gave software-based security methods in response to this question instead of physical. The most common responses included locking doors, CCTV and guards to physically prevent access to a computer.</p>
	b		<p>1 mark for each name, 1 per bullet for matching to description to max 2 each. e.g.</p> <ul style="list-style-type: none"> • Anti-malware <ul style="list-style-type: none"> ◦ Scans for / identifies virus/spyware/malware ◦ Compares data to a database of malware ◦ Alerts user and requests action such as .. ◦ Quarantines/deletes virus/spyware/malware ◦ Stops the download of virus/spyware/malware • Firewall <ul style="list-style-type: none"> ◦ Scans incoming and outgoing traffic ◦ Compares traffic to a criteria ◦ Blocks traffic that is unauthorised ◦ Blocks incoming/outgoing traffic • Encryption <ul style="list-style-type: none"> ◦ Scrambles data 	6	<p>Mark method first. If method is wrong, do not read on. If method is unclear, or part of a description of a method, read full answer.</p> <p>If second method is a repeat of the first (for example password and then locking out) mark whole answer for max 3.</p> <p><u>Examiner's Comments</u></p> <p>Many candidates answered this question well Strong responses correctly identified software-based security methods; most commonly anti-malware/anti-virus, firewalls, passwords and encryption.</p> <p>The descriptions of anti-malware, anti-spyware and anti-viruses were often</p>

			<ul style="list-style-type: none"> ○ ...using an algorithm ○ So if intercepted it cannot be understood ○ Key needed to decrypt • User access levels <ul style="list-style-type: none"> ○ Data can be read/write/ read-write / by example ○ Prevents accidental changes ○ Limits data users can access • Anti-virus <ul style="list-style-type: none"> ○ Scans for / identifies virus/malware ○ Compares data to a database of viruses/malware ○ Alerts user and requests action such as .. ○ Quarantines/deletes virus/spyware ○ Stops the download of virus/malware • Anti-spyware <ul style="list-style-type: none"> ○ Scans for / identifies spyware / keylogger ○ Compares data to a database of spyware ○ Alerts user and requests action such as .. ○ Quarantines/deletes spyware ○ Stops the download of spyware/malware • Passwords/biometrics/authentication <ul style="list-style-type: none"> ○ code/fingerprint etc. has to be correctly entered to gain access ○ strong password / letters, numbers, symbols / fingerprint is unique to individual ... ○ harder/impossible for a brute-force attack to succeed ○ lock after set number of failed attempts • Two-step authentication <ul style="list-style-type: none"> ○ a code is sent to user's separate device ○ unauthorised person will need access to this device as well 		stronger than those that gave firewalls and encryption.
			Total	8	

5			1 mark for each completed box	6	Enter text here.												
			<table><tr><th>Form of attack</th><th>Description of attack</th><th>Method of prevention</th></tr><tr><td>Brute-force attack</td><td>A program attempting all possible password combinations</td><td>Strong password / set number of password attempts / firewall</td></tr><tr><td>Data interception</td><td>Data transmission being read by unauthorised user/program</td><td>Encryption</td></tr><tr><td>Malware/Virus/Trojan etc.</td><td>Software that damages/deletes data</td><td>Anti-virus</td></tr></table>			Form of attack	Description of attack	Method of prevention	Brute-force attack	A program attempting all possible password combinations	Strong password / set number of password attempts / firewall	Data interception	Data transmission being read by unauthorised user/program	Encryption	Malware/Virus/Trojan etc.	Software that damages/deletes data	Anti-virus
			Form of attack			Description of attack	Method of prevention										
			Brute-force attack			A program attempting all possible password combinations	Strong password / set number of password attempts / firewall										
Data interception	Data transmission being read by unauthorised user/program	Encryption															
Malware/Virus/Trojan etc.	Software that damages/deletes data	Anti-virus															
Total			6														
6	a		<ul style="list-style-type: none">• Firewall (1 – AO2 1a) prevents unauthorised access (1 – AO2 1b)• Anti-malware (1 – AO2 1a) removes viruses/spyware from infecting the system (1 – AO2 1b)• Encryption (1 – AO2 1a) any intercepted data is rendered useless (1 – AO2 1b)• User access levels (1 – AO2 1a) users have restricted access (1 – AO2 1b)• Network policies (1 – AO2 1a) rules that define acceptable use (1 – AO2 1b)	6 AO2 1a (3) AO2 1b (3)	1 mark to be awarded for each correct type to a maximum of 3 marks. (AO2 1a) 1 mark to be awarded for each correct explanation to a maximum of 3 marks. (AO2 1b)												
			<ul style="list-style-type: none">• Brings in files via any medium (1 – AO2 1a)...• ...not allowing/stopping external devices being used on the network (1 – AO2 1b)• Downloading infected files from the internet (1 – AO2 1a)...• ...blocking/restricting access to insecure websites (1 – AO2 1b)• Allowing physical access to the surgery's network (1 – AO2 1a)...			6 AO2 1a (3) AO2 1b (3)	1 mark to be awarded for each correct identification to a maximum of 3 marks. (AO2 1b) 1 mark to be awarded for each correct outlining of a procedure to a maximum of 3 marks. (AO2 1b) Allow any reasonable										

			<ul style="list-style-type: none">• ...locking of doors/key cards/any physical security procedure (1 – AO2 1b)• Sending/sharing sensitive data with third parties (1 – AO2 1a)...• ... blocking/restricting access to USB ports/email/internet/printing (1 – AO2 1b)		combination of error and reasonable procedure to mitigate the risk.
			Total	12	