OCR
Oxford Cambridge and RSA

Cambridge Technicals
IT

Unit **3: Cyber Security**

Level 3 Cambridge Technical in IT

Mark Scheme for June 2018

OCR (Oxford Cambridge and RSA) is a leading UK awarding body, providing a wide range of qualifications to meet the needs of candidates of all ages and abilities. OCR qualifications include AS/A Levels, Diplomas, GCSEs, Cambridge Nationals, Cambridge Technicals, Functional Skills, Key Skills, Entry Level qualifications, NVQs and vocational qualifications in areas such as IT, business, languages, teaching/training, administration and secretarial skills.

It is also responsible for developing new specifications to meet national requirements and the needs of students and teachers. OCR is a not-for-profit organisation; any surplus made is invested back into the establishment to help towards the development of qualifications and support, which keep pace with the changing needs of today's society.

This mark scheme is published as an aid to teachers and students, to indicate the requirements of the examination. It shows the basis on which marks were awarded by examiners. It does not indicate the details of the discussions which took place at an examiners' meeting before marking commenced.

All examiners are instructed that alternative correct answers and unexpected approaches in candidates' scripts must be given marks that fairly reflect the relevant knowledge and skills demonstrated.

Mark schemes should be read in conjunction with the published question papers and the report on the examination.

Annotations - These are the annotations to be used when marking Unit 2:

Annotation	Meaning
	Tick – correct answer
	Cross – incorrect answer
	Plus – use for positives
	Minus – use for negatives
L1	Level 1
L2	Level 2
L3	Level 3
BOD	Benefit of doubt (This **does** count as a mark – so do not 'tick' as well)
^	Omission mark
V	Too vague
R	Repeat
 or 	Noted but no credit given

Section A

Question			Answer	Marks	Guidance
1	a		***Possible reasons why it is important for Mr. Daka to protect his personal information include:*** • Can lead to identify theft/fraud (1) can get enough information to persuade others they are him/if (example) date and place of birth are known/implication of identity theft (1). • Maintain his privacy (1) does not want all information about him revealed to public (1). • Protect his finances (1) could withdraw money from his account or equivalent (1). • Can lead to blackmail (1) if personal information could be exploited(1) • To prevent unauthorised access (by a third party)/hacking (1) so they do not misuse personal information(1) • Any other valid suggestion.	4	***Up to two marks for each of two explanations.*** One mark is for identifying a reason. Award ANY reasonable reason that shows why personal information should be protected (**this is an implication of the information being stolen not the initial protection**). Second mark is for explaining why/how it is a reason (candidate can identify the personal details that are lost as part of the "how"). Answer may be an implication of data theft, or deal with the theft in the first place (bullet point 5) Numbers on lines are for guidance only. Candidate may answer wholly within section 1, for example. Mark first two explanations ONLY DO NOT accept non-personal information – such as password or address
	b		***Possible pieces of information include:*** • Date of birth (1) • User name (1) • Online password to website (1) • Address (1) • When present/not present in the house (1) • Current status of any device controlled by the DPA (1) • Financial information (or examples thereof) (1) • Questions/searches (NOT activities) that have been asked (1) • Any other valid suggestion.	2	Should be realistic and available from a personal digital assistant. <u>However, information held on the DPA can includes shopping lists, to do lists etc</u>. For password, allow specific examples DO NOT allow: • Medical records • Personal information • Current location

Question			Answer	Marks	Guidance
	c		***Possible pieces of information include:*** • IP/MAC address of router/equivalent device (1) • Password/passcode (1) • Username (1). • Version of software (1). • Any other valid suggestion.	2	***For two marks:*** Allow information relating to Mr. Daka, the network, or the device. Allow any reference to password/passcode.
	d		**Possible methods an attacker could use to get personal information directly from Mr. Daka include:** • Social engineering (1) pretending to be from bank/software company (1) • Pharming (1) user directed to fake website (1) • Phishing (1) email claiming to be from an authority/bank etc/demand for personal information (1) • Scamming (1) use of fraudulent means (or example)/encourages installation of malware (1) • Spyware (1) which records key strokes (1) • Gain access to security cameras (1) to read bank card details (1) • Any other valid suggestion.	4	***Up to two marks for each of two descriptions.*** One mark for method (accept NOUN or VERB). Method may be passive OR active. Another mark for description of that method. NB does not need to state the type of personal information accessed/got. Attack MUST be a cyberattack. DO NOT accept attacks which are <u>clearly</u> physical. DO NOT accept “hacking” e.g. “Hacking by <u>cracking a wifi password</u>” – 1 mark for underlined portion of answer only

Question			Answer	Marks	Guidance
	e		***Possible ways a cyber-attack on the digital personal assistant could result in a physical vulnerability to his property include:*** • Turning the heating off (1) can lead to frozen pipes (1) • Door can be opened remotely (1) allowing access to property (1) • Alarm systems can be switched off (1) so if a break in occurs they will not go off (1) • Cameras/microphone can be accessed (1) to see if Mr. Daka is at home (1). • Create a power surge (1) so that fuse board/router trips (1) • Any other valid suggestion.	4	***Up to two marks for each of two explanations.*** Needs to involve something <u>physical occurring at/to the property</u>, not just data. Expansion must explain the physical vulnerability. For example – change door pass code (1) so that the house can be burgled (1) Do not award expansions which deal with after the event consequences (such as delete camera recording so that evidence of robbery deleted).
2	**a**		***Possible responses include:*** • Individual who sells information (1st) • To a third party/example (1) • Information includes flaws in a device/how to access device (1) • Information on how to hack into the device (1) • Any other valid suggestion (1)	2	***Up to two marks for description.*** Answer must clearly deal with the broker selling information that is found. This is NOT the same as being employed to identify issues. Expansion must be more than simply stating “about vulnerabilities”. Must be an example of.

Question			Answer	Marks	Guidance
	b		***Possible reasons why Mr. Daka should be concerned by a vulnerability broker having information about the digital personal assistant include:*** • The broker needs (issues to sell) (1) (if he has found them) means there is a flaw in the system (1) multiple individuals can buy the flaw and gain access (1) • Company has not fully tested the product (1) might be other issues with the technology (1) • Broker can sell/pass on the information (1) one implication (1) • Any other valid suggestion.	4	***Up to two marks for each of two descriptions.*** Answers must be about the fact that the vulnerability broker has obtained the data (- such as Why? How?) Vulnerability broker who uses the data themselves is not a VB by definition.
	c		***Possible motivations include:*** • To gain personal information (1st) that can be used in a crime (1) such as identity theft (1). • Public Good (1st) raising awareness of a vulnerability so company can patch it (1) reducing opportunities for hacking (1). • Thrill (1st) finding out if the device can be hacked (1) beating fellow hackers to find the vulnerability (1) • Blackmail (1st) use of information (1) to make Mr Daka do something he would rather not do (1) • Personal vengeance (1st) negative impact on Mr Daka (1) to redress some previous hurt (1) • Havoc and mayhem (1st) to cause disruption (1) for a personal thrill (1) • Publicity (1st) name becomes known (1) for deep joy (1) • Any other valid suggestion.	6	***In each of two cases:*** Need to identify motivation <u>before</u> description marks can be awarded Do not allow income generation of any type as an example OR expansion (fraud is acceptable, as can lead to personal gain)

Question			Answer	Marks	Guidance
	d		***Possible responses include:*** • If all devices have the same vulnerability (1) allows access to many devices with same hack (1) do not have to spend time researching/running each hack (1). • Large number of homes/devices (1) with the same vulnerability (1) makes it easier to blackmail/extort money **from developer/**earn money (1). • Any other valid suggestion.	3	***Up to three marks for explanation.*** Answers must deal with an **attack on the brand**, rather than an attack on an individual DPA.
3	a		***Possible areas that should be examined for security vulnerabilities that are dependent on Mr. Daka's network and not the digital assistant include:*** • Access controls (1) which accounts have access to which parts of the system/ level of access of different accounts (1). • Wifi security (1) encryption enabled/ssid hidden (1). • Default settings (1) have they been changed (1). • Open ports (1) which ports on the router are open/available (1) • Firewall (1) to check that it is checking all/any traffic (1) • Any other valid suggestion.	4	***Up to two marks for each of two descriptions.***
	b		***Possible responses include:*** • Overload the system with data (1st) • See how it responds/make sure it does not crash/check whether does crash (1). • Any other valid suggestion.	2	***Up to two marks for description.***

Section B

Question			Answer	Marks	Guidance
4	a		***Possible responses include:*** • HIDS – installed on every network computer (1) NIDS - only installed at specific points (1) • HIDS - all devices with two way access to external environment (1) • NIDS - installed on devices that sit between network and external environment (1) • HIDS - only examines traffic directed at host/single computer it is protecting (1) • NIDS – examines all traffic (1). • Any other valid suggestion.	2	***Up to two marks for description.*** Can award one mark for a statement about either system. For full marks, must be a comparison, not two individual unrelated statements
	b*		**Indicative content:** • There are different types of IDS which can provide different functions, no single IDS will provide all functions meaning that either multiple IDS need to be run using resources or there may be gaps in the functionality. • Alarms are raised in real time but this requires a network operator to be available and monitoring in order to react. • Hacker may use signatures (for example) that are matched within the rule base and so will not raise the alarm. • Signatures cannot be detected if they are not in the rule base only making them useful for attacks that have happened elsewhere. • False positives can be flagged wasting investigation time. • IDS continue to improve over time as signatures continually added to the IDS model. •	10	**Mark Band 3 (7-10 marks)** The learner has explained the advantages and disadvantages of using an IDS as a method for protecting a network. Both sides of the argument are considered with some attempt to prioritise the information that is given. Subject specific terminology and knowledge will be clearly used to support and inform the explanations. *There is a well-developed line of reasoning which is clear and logically structured. The information presented is relevant and substantiated.* **Mark Band 2 (4-6 marks)** The learner has described how an IDS might be used to protect a network. There is some consideration of advantages and/or disadvantages. At the bottom end of this mark band, the learner may give a generic description of how an IDS works. *There is a line of reasoning presented with some structure. The information presented is for the most part relevant and supported by some evidence.*

Question			Answer	Marks	Guidance
			• IDS look for known weaknesses, these can be avoided by hackers. • Any other valid suggestion		**Mark Band 1 (1-3 marks)** The learner has identified generic points in relation to an IDS. Subject specific terminology may be limited or missing. The information is basic and communicated in an unstructured way. The information is supported by limited evidence and the relationship to the evidence may not be clear. **0 marks** = Nothing worthy of credit.

Question			Answer	Marks	Guidance
5	a		***Possible ways SafeWithUs could determine the capability of the attackers include:*** • Time they spent in the system (1st) this will determine if they knew what they were doing/structure of the system (1). • Examine any logs for where accessed/what could not access (1st) to identify the levels of security that they could not beat (1) • What trail was left behind (1st) to identify effectiveness/efficiency (1) • Consider security used on the network (1st) to identify/gauge the level of security overcome (1) • Any other valid suggestion.	4	***Up to two marks for each of two descriptions.*** Do not allow techniques used/type of hacking. This is not about the level of capability but how to find it out. DO NOT accept location/country of origin
5	b		**Indicative content:** ***Possible reasons why SafeWithUs needs to understand the techniques used by the attackers include:*** • Profiling the attacker so that this individual/type of attacker can be protected against • To know how the attacker got in so that the vulnerability can be repaired and not exploited again. • To know which part of the system were accessed by the attacker which will help them identify which data was accessed/compromised so customers/authorities can be notified. • To know if it is the result of a script kiddie/vulnerability broker or if it is a new hack and they need to inform the hardware manufacturer. • To determine where responsibility lies within the company and if any law has been broken, such as the DPA. • Any other valid suggestion.	7	**Mark Band 3 (5-7 marks)** The learner has explained reasons why SafeWithUs needs to understand the techniques used by the attackers **Mark Band 2 (3-4 marks)** The learner has described how the technique**s** used by attackers may inform the decisions taken by SafeWithUs around cyber security. **Mark Band 1 (1-2 marks)** The learner identifies generic points in relation to why knowledge of techniques used by attackers are important. **0 marks** = Nothing worthy of credit.

OCR (Oxford Cambridge and RSA Examinations)
The Triangle Building
Shaftesbury Road
Cambridge
CB2 8EA

OCR Customer Contact Centre

Education and Learning
Telephone: 01223 553998
Facsimile: 01223 552627
Email: general.qualifications@ocr.org.uk

www.ocr.org.uk

For staff training purposes and as part of our quality assurance programme your call may be recorded or monitored

Oxford Cambridge and RSA Examinations
is a Company Limited by Guarantee
Registered in England
Registered Office; The Triangle Building, Shaftesbury Road, Cambridge, CB2 8EA
Registered Company Number: 3484466
OCR is an exempt Charity

OCR (Oxford Cambridge and RSA Examinations)
Head office
Telephone: 01223 552552
Facsimile: 01223 552553