Oxford Cambridge and RSA

Cambridge Technicals
IT

Unit 3: Cyber Security

Level 3 Cambridge Technical in IT
05838 – 05842/05877

Mark Scheme for January 2020

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.

Abbreviations, annotations and conventions used in the detailed Mark Scheme (to include abbreviations and subject-specific conventions).

Annotation	Meaning
x	Wrong
✓	Correct
L1/L2/L3	Level of Response
REP	Repetition of point

<table>
<tr><th colspan="3">Question</th><th>Answer</th><th>Marks</th><th>Guidance</th></tr>
<tr><td>1</td><td>(a)</td><td></td><td>Correct answers only, one per row

<table><tr><td>Scenario</td><td>Type of Attack</td></tr><tr><td>Burst water pipe in the server room</td><td>Environmental (1)</td></tr><tr><td>ID Access card being stolen</td><td>Physical (1)</td></tr><tr><td>Brute force password hack</td><td>System (1)</td></tr></table></td><td>3</td><td></td></tr>
<tr><td></td><td>(b)</td><td>(i)</td><td>2 marks for each, for example:
Public good:
• To ensure systems are safe (1) for the customers (1)
• To force the company (1) to increase their protection of data/realise how vulnerable they are (1)
• To find the vulnerabilities (1) before they can be used for fraud (1)
• To show how easy it is to hack (1) and customer should go elsewhere (1)
• To find information (1) e.g. illegal practices (1)
• E.g. Company is selling personal data to insurance companies (1)
Righting perceived wrongs:
• Finding information (1) to help support an individual/incriminating data (1)
• Making public information (1) that the hacker feels should not be hidden (1)
• Using skills to assist (1) those without them who have been wronged (1)</td><td>6</td><td>Allow max one example related to the case study for each

Score settling: who and why, must infer retaliation</td></tr>
</table>

Question			Answer	Marks	Guidance
			• "David and Goliath" mentality (1) on behalf of another individual (1) • An avenging angel/getting revenge (1) because the physiotherapist is committing an illegal/immoral act on their patient (1) • E.g. Company has not given out all records it has to do with a court case (1) Score settling: • Disgruntled employee/individual (1) who wants revenge (1) • Punishing the company (1) for something that has been done to them (1) • Rival company (1) who has lost business to Fairest (1) • E.g. an employee fired for stealing takes customers credit card details (1)		
		(ii)	2 from, for example: • Potential weak system (1) easily hacked to get usernames and passwords (1) • State hacks companies in its own country (1) to improve (nations) cyber security (1) • General information gathering (1) • Get an idea of the health of the nation (1) • If the clinic is having information about someone in the power like president (1), they might leak this information (1)	2	Allow any reasonable answer State could refer to home state or abroad

<table>
<tr><th colspan="3">Question</th><th>Answer</th><th>Marks</th><th>Guidance</th></tr>
<tr><td></td><td>(c)</td><td>(i)*</td><td>Indicative content:

• Loss of customer data which breaches DPA regulations;
• Loss of customer confidence which could lead to customers moving to a different company so the physiotherapist could close.
• Legal action if it is determined that the source of the hack is something that could have been prevented and the responsibility of the company – to changing default passwords for example.
• Enables policies and procedures to be tested and for all members of staff to understand their responsibilities

Impact is on physiotherapist business NOT the customer</td><td>10</td><td>
<table>
<tr><td>7 – 10 marks</td><td>Has analysed (explained) the impact of the cyber security attack on Fairest Physiotherapy.

There are clear impacts given which are in turn supported by examples.

Ideas will be expressed clearly and fluently.

There is a well-developed line of reasoning which is clear and logically structured. The information presented is relevant and substantiated.</td></tr>
<tr><td>4 – 6 marks</td><td>Has described the impact of the cyber security attack on Fairest Physiotherapy.

The supporting argument may be lacking the use of examples, or where examples have been used, these are not used strongly, or the supporting argument may be poorly developed and lacking in detail.

There will be a line of reasoning presented with some structure. The information presented is in the most part relevant and supported by some evidence.</td></tr>
<tr><td>1 – 3 marks</td><td>Has identified some points relevant to Fairest Physiotherapy being hacked.

There may be examples, but these are not used as part of a coherent answer.

The information is basic and is communicated in an unstructured manner. The information is supported by limited evidence and the relationship to the evidence may not be clear.</td></tr>
<tr><td>0 marks</td><td>Nothing worthy of credit</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th colspan="3">Question</th><th>Answer</th><th>Marks</th><th>Guidance</th></tr>
<tr><td></td><td></td><td>(ii)*</td><td>Indicative content:
• Employ an ethical hacker/external company to determine the weak points in the system
• Employ a social engineering company to pretend to be a customer and phone in to obtain personal information. Use of different techniques – e.g. crying baby to gather information.
• Conduct a physical review of the offices looking at position of monitors and what can be seen and what information can be gathered that could be used in a hack.
• Employ a third party consultant to examine the policies and procedures and then go undercover to see if they are being implemented as policies that are not being followed are a potential weak point in a system.
• Monitor/increased/abnormal levels of traffic in key areas, this could be done by installing a firewall and looking at the logs.

NOT about actions to take to protect the network.
This is about actions to FIND vulnerabilities.</td><td>7</td><td>
<table>
<tr><td>5-7</td><td>Has shown a detailed level of understanding by explaining how the areas at risk can be identified.
The candidate is able to provide a clear explanation of more than one action associated risk
Relevant examples will be used to support evaluation and ideas will be expressed clearly and fluently.
There is a well-developed line of reasoning which is clear and logically structured. The information presented is relevant and substantiated</td></tr>
<tr><td>3-4</td><td>Has shown a good level of understanding by describing how areas could be identified.
Explanations may have limited depth in the expansions.
Some examples used to support explanation may not be relevant and may at times detract from fluency of narrative.
There will be a line of reasoning presented with some structure. The information presented is in the most part relevant and supported by some evidence</td></tr>
<tr><td>1-2</td><td>Has identified areas of the company that are at risk.
Limited use of examples to accompany description and ideas will be poorly expressed.
The information is basic and is communicated in an unstructured manner. The information is supported by limited evidence and the relationship to the evidence may not be clear.</td></tr>
<tr><td>0</td><td>Nothing worthy of credit</td></tr>
</table>
</td></tr>
</table>

Question			Answer	Marks	Guidance
		(iii)	2 marks for each measure, for example: • Act immediately (1) any concerns should be addressed straightaway (1) • Removing customer data (1) to offline so not accessible (1) • Prevention (1) finding out how the hacker got in and sealing the entry point (1) • Communication (1) letting customers know what has happened (1) • Publicity (1) rebuilding reputation/appointment of high profile team (1)	6	This is about reducing the impact of the hack and **not** stopping the hack itself. This is AFTER a hack has occurred NOT before Max 2 (one measure only) for prevention
2	**(a)**		4 from for example: • To stop it being accessed (1) by unauthorised personnel (1) • If hacked (1) then backup will not be lost as well (1) • To prevent financial payment information being released (1) and customers defrauded (1) • Backup contains personal information (1) to meet the requirements of the law/ DPA(1)	4	
	(b)		2 from, for example: • In case data is accidentally deleted / lost (1) it be restored/replaced (1) • In case they get a virus (1) and need to go back to a version that was clean (1) • If the system was destroyed (1) by fire/flood (1)	2	

Question			Answer	Marks	Guidance
3			1 mark for each item to a max 3, 1 mark for each reason to a max 3, for example: • Item: Bank account number (1) • Reason: So the company can identify which account has been hacked (1) • Item: Proof of identity (1) • Reason: So they know they are communicating with the account holder (1) • Item: Time/date of hack (1) • Reason: To know which logs to look at (1) • Item: Amount taken (1) • Reason: To track the amount through the system / look for patterns in other hacks of accounts (1)	6	These are examples only. Any reasonable item of information needed by the bank and why they need it / how they would use it. The reason can be the same with different information The reason cannot be awarded without the item
4			3 from, e.g. • Financial data (1) • National Insurance data (1) • Employment data (1) • Pension Data (1)	3	Do not allow examples of data but allow different categories of the same type – e.g. financial/pension **Not** an item of information **Not** health/medical data

Question			Answer	Marks	Guidance
5	(a)		1 mark each, for example: Data at rest: • Inactive data / data in one place / data that can be accessed / e.g. data in a database (1) Data in transit: • Data being transferred / Data moving from one device to another (1) In the cloud: • Data stored off site / using third party servers / logical pools of data (1)	3	
	(b)		2 from, for example: • Steganography (1) • Hash functions (1) • Public key (1) • Private key (1) • Symmetric (1) • Asymmetric (1) • Secret key cryptography (1) • Passwords (1) • Encryption (1) • WPA / WPA2 (1)	2	Allow examples, for example Caesar Cypher.

Question			Answer	Marks	Guidance
6	(a)		4 from: for example: • To prevent hackers (1) exploiting the vulnerability/gaining personal data (1) • Keeping the data secure (1) • Making sure the system is protected (1) • Complies with legal requirements (1) • Prevents the software causing further issues, system crash, temporary glitches(1) • May help solve issues that Paulina has been having (1) • Improve performance of the software (1)	4	
	(b)		2 from, for example: • Patch repairs an error (1) • Update adds functionality (1)	2	

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