www.xtrapapers.com

OCR
Oxford Cambridge and RSA

Cambridge Technicals
IT

Unit **3: Cyber Security**

Level 3 Cambridge Technical in IT

Mark Scheme for June 2017

www.xtrapapers.com

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.

OCR will not enter into any discussion or correspondence in connection with this mark scheme.

© OCR 2017

Section A

Question			Answer	Marks	Guidance
1	(a)		Two marks, one for example e.g. • Information is accessible when required (1) e.g. booking information on customers when they book in (1) • Only accessible to authorised viewer (1) e.g. only receptionists can see credit card details of customers. (1) • How easy it is for a person to access the data you need (1) such as front desk staff checking bookings (1)	2	**If no example then max 1 mark**
	(b)	(i)	Two from e.g. • So they know when they are at the hotel (1) so they can rob the house (1) • So they can gain access to their card/bank details (1) and steal money (1) • Can use information for criminal activities (1) such as identity theft (1)	2	The answer needs to be more than the information they would gain but why they would want it.
	(b)	(ii)	Four marks. e.g. • Staff (1) credit card details (1) used to impersonate an individual (1) and steal money (1) • Web host (1) credit card details(1) used to impersonate an individual (1) and steal money (1) • Suppliers (1) identity of delivery drivers (1) to know who to impersonate (1) to gain physical access to the hotel (1) • Equipment (1) passwords (1) to gain access to computer	4	The identified target must have something to do with the hotel. Do not allow customers. Target must be within the hotel, not the hotel itself. Target and use must be linked.

Question			Answer	Marks	Guidance
			system (1) to steal address details (1)		

<table>
<tr><th colspan="3">Question</th><th>Answer</th><th>Marks</th><th>Guidance</th></tr>
<tr><td>2</td><td>(a)</td><td>*</td><td>Indicative content:
• They might try and spend on their credit cards but find that there is not credit – might not be able to purchase the items/have to return them – leads to embarrassment.

• Identity theft – their details can be stolen and someone can impersonate them, running up debts, destroying credit history and making it difficult for them to buy items/mortgages in the future.

• The location is known on certain dates which means that they are not at home which will be empty so hackers can arrange for it to be broken into.</td><td>10</td><td>Level of response marking:

<table>
<tr><td>7 - 10 marks</td><td>Candidate has shown a detailed level of understanding by discussing impacts on the customers.
Relevant examples will be used to support discussion 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>4 – 6 marks</td><td>Candidate has shown a good level of understanding by explaining at least one impact on the customers.
Some examples will be used to support the explanation which may not be relevant and may at times detract from fluency of narrative.

At the bottom end of the mark band, the candidate may have described a single impact.

There is 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>Candidate has identified points relevant to impacts of the theft of customer data.
Limited use of examples to accompany the description and ideas will be poorly expressed.
At the bottom end of the mark band, a</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></td><td></td><td></td><td>
<table>
<tr><td></td><td>single impact may be identified with an example.
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.</td></tr>
<tr><td>0 marks</td><td>Nothing worthy of credit.</td></tr>
</table>
</td></tr>
<tr><td></td><td>(b)</td><td></td><td>Two marks for a full explanation of the impact on each stakeholder.
e.g.
• Shareholders/owners will suffer as the share price will fall (1) as there is a lack of confidence as customers will not book in the future (1)
• Employees may be made redundant (1) as bookings will be cancelled as customers move to a different hotel (1)
• Network manager may not be able to get another job (1) as his reputation for allowing a cyber security attack may follow him (1)</td><td>4</td><td>Answer is about the impact, not who the stakeholder is. Therefore, stakeholder does NOT have to be mentioned.

Accept internal and external stakeholders:

e.g.
• Suppliers
• Competitors

Accept wider implications, such as reputation impacts and motivation of key staff.</td></tr>
</table>

3	**(a)**		Two marks per section: Title: • To identify the (focus of the) report (1) to find it for future reference when filed (1) Target: • To show what data was targeted/stolen (1) to see if there is a pattern in the targets attacked (1) to identify vulnerabilities that can be prevented/make improvements (1)	4	
3	**(b)**		Two marks for each description: e.g. • [by examining] Logs (1) detailing ports used (1) • Observation / watching on CCTV (1) looking at the route used to gain access (1) • Interview/talk to (1) talking to targets of the hack (1) • Customer incident reports (1) showing what information was stolen/when the attack occurred (1) • Proforma/questionnaire (1) gathers data about the attack (may give examples) (1)	4	Must be a description of a method, with method identified (no method – no mark).

	(c)		Two marks for a full explanation e.g. • Will identify areas for improvement (1) to prevent the attack happening again (1) • To allow an action plan to be completed (1) addressing the issues identified (1) • Those who are affected can be contacted and reassured about the security of their data (1) limiting the implication of the attack (1) • To understand the extent of the attack (1) so can gauge severity of the attack (1)	2	

<table>
<tr>
<td>4</td>
<td>*</td>
<td></td>
<td>Indicative content:
• Will find the security gaps that can then be closed meaning that “real” hackers will not be able to use them to gain access to OCR Hotel’s computer systems.

• Will enable the Hotel staff to focus on preventing attacks rather than having to learn new skills to try and gain access themselves.

• Ethical hacker may find gaps in security that they do not notify the hotel about and use/sell them to other people to utilise.

• May be seen as a negative move by customers or shareholders as may mean that they think they are vulnerable.</td>
<td>7</td>
<td>
<table>
<tr><td>5 - 7 marks</td><td>Candidate has shown a detailed level of understanding and has evaluated the implications to OCR Hotels in detail.

Relevant examples will be used to support discussion and ideas will be expressed fluently.</td></tr>
<tr><td>3 – 4 marks</td><td>Candidate has shown a good level of understanding and has explained the implications to OCR hotels, although the explanations may be one sided.

Examples will be used to support explanations which may not be relevant and may at times detract from the fluency of the narrative.

At the bottom end of the mark band, the candidate may have described a single implication.</td></tr>
<tr><td>1 – 2 marks</td><td>Candidate has identified implications to OCR Hotels.

There will be limited (if any) use of examples to accompany the points made and ideas will be poorly expressed.

At the bottom end of the mark band, a single point may be identified.</td></tr>
<tr><td>0 marks</td><td>Nothing worthy of credit.</td></tr>
</table>
</td>
</tr>
</table>

Section B

Question			Answer	Marks	Guidance
5	**(a)**		Two from, two marks each, e.g. • Black box/blind testing (1) where the tester is not given any information about the workings of the system (1) • Firewall configuration testing (1) checking the settings on the firewall/different to default/set correctly (1) • Social engineering (1) phoning employees to try and gain passwords (1)	4	Allow generic answers based on internal/external/blind/double blind/black box/white box. Grey box testing as well as specific examples of individual tests.
	(b)		Up to three marks for each answer: First mark – Reason Second and third mark – explanation of reason e.g. • They are highly trained at what they do/more skills than the individual (first) • Will do a better job than the individual (1) because more likely to identify issues (1) Answer may also be about outcome the tests and why these outcomes occur • The company will be able to test for weak points in the network (1) (first) • And report these back to the individual (1) so that they can be	6	Answer may also be about outcome the tests and why these outcomes occur

Question			Answer	Marks	Guidance
			rectified (1)		

Question			Answer	Marks	Guidance
5	(c)		One mark for identification of control, max two for how it prevents, e.g. • Biometric access (1) coded to an individual (1) hard to duplicate/which are unique (1) • Alarm (1) notifies others of an intrusion (attempt) (1) so that the break in can be investigated (1) • Cable locks (1) prevent the computer from being physically removed (1) by attaching it to a fixed item (1) • Safe (1) prevents access to the data (1) different set of skills required to access data in the safe (1)	6	Answer MUST be about the security control and NOT the implication
6	(a)		Two from e.g. • Stealing credit card details/credit card details (1) • Selling the data on (1) • Identify theft (1) • Ransomware (1)	2	"Steal personal details" on its own is too vague. However, if candidate identifies two items of personal data which together could enable identity to be stolen, award identity theft mark point
	(b)		One from: • Storing data in a form that only those with a key can read and process it (1) • Use of encryption and decryption to prevent data from being understood if intercepted (1)	1	
	(c)		One from: e.g. • Delete the data (1)	1	DO NOT accept "copy data" DO NOT accept "encryption"

Question			Answer	Marks	Guidance
			• Physically breaking the computer/hard drive (1) • Change passwords (1) • Move data (1)		

www.xtrapapers.com

OCR (Oxford Cambridge and RSA Examinations)
1 Hills Road
Cambridge
CB1 2EU

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; 1 Hills Road, Cambridge, CB1 2EU
Registered Company Number: 3484466
OCR is an exempt Charity

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

© OCR 2017

PART OF THE CAMBRIDGE ASSESSMENT GROUP

LLOYD'S REGISTER QUALITY ASSURANCE · ISO9001 · UKAS MANAGEMENT SYSTEMS 001