OCR
Oxford Cambridge and RSA

SAMPLE ASSESSMENT MATERIAL

Level 3 Cambridge Technical in IT
05839/ 05840/ 05841/ 05842
Unit 3 Cyber security

Date – Morning/Afternoon
Time Allowed: 1 hour

You must have:

- The Insert (clean copy case study)

First Name						Last Name				
Centre Number						Candidate Number				
Date of Birth										

INSTRUCTIONS
- Use black ink.
- Complete the boxes above with your name, centre number and candidate number.
- Answer **all** the questions.
- Write your answer to each question in the space provided.
- Do **not** write in the bar codes.

INFORMATION
- The case study should be used to answer questions in Section A.
- The total mark for this paper is **60**.
- The marks for each question are shown in brackets **[ ]**.
- Quality of extended response will be assessed in questions marked with an asterisk (*).
- This document consists of **12** pages.

Answer **all** the questions.

Section A

This section relates to the case study.

1

(a) Describe what is meant by the term *integrity of data* in the context of data and network security.

……

……

……

…… **[2]**

(b) Describe **one** way in which integrity of data could be compromised at Classic Cars.

……

……

……

…… **[2]**

(c)

(i) Identify **two** types of attacker, working alone, who would be interested in compromising the computer networks at *Classic Cars*.

1. ……

2. ……
[2]

(ii) For **one** of the attackers, identified in part (c)(i), identify **two** of their characteristics.

Name of attacker: ……

1. ……

2. ……
[2]

(iii) Explain **one** possible motivation for the attacker identified in part (c)(ii).

……

……

……

……

……

…… **[3]**

2

(a) Identify **two** vulnerabilities that have the potential to be exploited at Classic Cars.

1. ……

2. …… **[2]**

(b) Describe **one** example of an attack that could be performed against the networks at *Classic Cars*.

……

……

……

…… **[2]**

(c)* Discuss possible impacts on *Classic Cars* of network security being breached.

……

……

……

……

[10]

3

(a) Recommend **two** software controls and **two** procedural controls that *Classic Cars* should use.

Write your answers in the box below:

Software controls	Procedural controls
1.	1.
2.	2.

[4]

(b) Describe **one** measure that *Classic Cars* should take to prevent information on external devices being accessed without authorisation.

……

……

……

…… **[2]**

(c) Identify **one** reason why *Classic Cars* should use an intrusion detection system on its network.

…… **[1]**

4

(a) The IT technicians at *Classic Cars* have identified malware on their network.

Explain **one** action they should take in response.

……

……

……

……

……

…… **[3]**

(b) Choose **one** category from the list below that describes the incident of the stolen external drive described in the case study.

Enter a tick in the box next to your choice.

Critical	
Significant	
Minor	
Negligible	

[1]

(c) Justify your choice of category in part 4(b).

……

……

……

……

……

……

……

…… **[4]**

Section B

You do not need the case study to answer these questions.

5

(a) Describe **one** potential cyber security issue associated with connecting your tablet or laptop to an unsecured Wi-Fi hotspot.

……

……

……

…… **[2]**

(b) * Evaluate the preventative measures you could take when connecting your tablet or laptop to an unsecured Wi-Fi hotspot.

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

…… **[8]**

6

A member of your family has received the email shown below; it appears to have been sent from the IT Support Team of the organisation with whom they have an email account.

Dear Sir/Madam,

We have decided to delete inactive email accounts to create space for new email accounts. In order to continue using your email account you must send us the information listed below.

If we do not receive this information from you immediately, your email account will be terminated.

Surname:
First name:
Email username:
Email password:
Date of birth:
Alternative email address:

Click on the link at the end of this message to enter your information

Please do not contact the IT Support department with any questions as we are too busy to respond. If you need further information, see the file attached to this email.

(a) State what type of email this is likely to be.

…… **[1]**

(b) Identify **three** items in the email that suggest that this is not a genuine email.

1. ……

2. ……

3. ……

[3]

(c) Evaluate the likely impact on your family member if they were to click on the link in the email.

……

……

……

……

……

……

……

……

……

……

……

…… **[6]**

END OF QUESTION PAPER

THIS PAGE HAS BEEN LEFT INTENTIONALLY BLANK

THIS PAGE HAS BEEN LEFT INTENTIONALLY BLANK

THIS PAGE HAS BEEN LEFT INTENTIONALLY BLANK

OCR
Oxford Cambridge and RSA

SPECIMEN

SAMPLE ASSESSMENT MATERIAL

Cambridge Technicals in IT

UNIT 3 Cyber security

MARK SCHEME

Duration: 1 hour

MAXIMUM MARK 60

Version: 1

Date: 31/07/2015

Section A

Question			Answer	Marks	Guidance
1	(a)		• Modification/change of data (1) without authorisation (1).	2	*Points marking approach.* *Up to two marks for valid* description.
	(b)		• Financial data could be modified/changed (1) as the permissions are not set to ensure managers have only read only access (1). • Employees are allowed to use their own mobile devices (1) which could result in the data being lost (1) or accessed by unauthorised personnel (1). • Any other valid suggestion.	2	*Points marking approach.* *One mark for correct identification plus an additional one mark for valid description.*
	(c)	(i)	• Hacker (1) • Employee (1) • Former employee (1) • Criminal (1) • Hacktivist (1) • Any other valid suggestion.	2	*Points marking approach.* *One mark for each correct identification up to a maximum of two identifications.*
	(c)	(ii)	• Hacker: any age (1), any social background (1), opportunist (1), intends to exploit vulnerabilities (1), uses various methods (1). • Employee: current (1), contractor (1), work experience (1). • Former employee: now works for a competitor (1), fired (1), contractor (1), work experience (1) • Criminal: any age (1), any social background (1), could be working on behalf of someone else	2	*Points marking approach.* *One mark for each correct identification up to a maximum of two identifications.*

Question			Answer	Marks	Guidance
			(1), uses various methods (1). • Hacktivist: any age (1), any background (1), uses various methods (1).		
	(c)	**(iii)**	• Hacker: to take control of the network (1), financial theft (1), data theft (1), theft of the blueprint (1), malware (1), denial of service (1), spy for a competitor (1), etc. • Employee: financial theft (1), data theft (1), theft of the blueprint (1), malware (1), industrial espionage (1), etc. • Former employee: financial theft (1), data theft (1), theft of the blueprint (1), malware (1), spy for a competitor (1), damage the network (1), revenge (1), challenge (1), etc. (1). • Hacktivist: to protest against the organisation (1), to make a political point (1), to cause disruption (1).	3	*Points marking approach.* *One mark for correct identification plus an additional two marks for valid explanation.*
2	**(a)**		• Staff using their own devices (1) • Cloud storage (1) • Wireless network (1) • Video conferencing (1) • Remote access (1) • Staff accessing the system from home (1) • Network hardware (1) • Network software (1) • Any other valid suggestion.	2	*Points marking approach.* *One mark for correct identification up to a maximum of two identifications.*
	(b)		• Key logging (1) where an attacker will be able to identify passwords (1). • Spam (1) where an attacker could flood the	2	*Points marking approach.* *One mark for correct identification plus an additional one marks for valid description.*

<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>network with emails (1) and could potentially introduce viruses/malware (1).
• Botnet (1) where an attacker could instigate an infection of malicious software (1) unbeknown to the company (1) in order to control their network (1).</td><td></td><td></td></tr>
<tr><td></td><td>(c)*</td><td></td><td>Indicative content:
• Reputation of the organisation could be damaged.
• Customers could lose confidence in the organisation and take their custom elsewhere.
• Business could be disrupted.
• Loss of business - the organisation could lose so much business that it goes into administration.
• Expense - it could cost the organisation a considerable amount of money.
• Staff morale could be affected adversely.
• Data loss - financial, personal.
• Competitors could gain an advantage.
• Any other valid suggestion.</td><td>10</td><td>Levels of response marking approach.
<table><tr><td>7-10 marks</td><td>Has shown a detailed level of understanding by discussing the impacts on Classic Cars if network security is breached. The learner is able to provide a clear explanation of more than one impact and the consequence of these impacts. 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>Has shown a good level of understanding by explaining the impact(s) on Classic Cars if network security is breached. Explanations may concentrate on either the impact or the consequence with 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 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></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>1-3 marks</td><td>Has identified points relevant to impacts on organisations if network security is breached Limited use of examples to accompany description and ideas will be poorly expressed.

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>3</td><td>(a)</td><td></td><td>Software controls
• Firewalls (1)
• Anti-malware (1)
• Operating system updates (1)
• Patch management (1)
• Anti-spyware (1)
• Any other valid suggestion.

Procedural controls
• Access management (1)
• User accounts and permissions (1)
• Data backup (1)
• Remote working (1)
• Device management (1)
• Awareness (1)
• Training (1)
• Any other valid suggestion.</td><td>4</td><td>Points marking approach.

One mark for each correct identification up to a maximum of four identifications.</td></tr>
<tr><td></td><td>(b)</td><td></td><td>• Encryption (1) would prevent unauthorised access to the information (1) as the information could be not be read (1).
• Any other valid suggestion.</td><td>2</td><td>Points marking approach.

One mark for correct identification plus an additional one marks for valid description.</td></tr>
</table>

Question			Answer	Marks	Guidance
	(c)		• To monitor the network (1) • To alert to a security incident (1) • To help to assess risks (1) • Reports unusual patterns/behaviour (1) • Monitors the system's resources (1) • Any other valid suggestion.	1	*For one mark:*
4	**(a)**		• They could contact the Incident Response Team (1). The team will prioritise the incident (1) to contain the malware (1). • The IRT will identify and mitigate vulnerabilities (1), eradicate the malware (1) and disinfect the network (1). • The ITR will confirm the system is functioning normally after the incident (1). A cyber security incident report will be produced (1), which will facilitate a review and evaluation of the incident (1). • Any other valid suggestion.	3	*Points marking approach.* *One mark for correct identification plus an additional two marks for valid explanation.*
	(b)		• Significant (1)	1	*For one mark:*
	(c)		• Customer/supplier/staff personal data could be compromised (1) resulting in identity theft (1), potential legal action (1) and loss of supplier and customer confidence (1). • Blueprint of the new car has been stolen (1). This will result in loss of competitive advantage (1) and loss of income to Classic Cars (1) as it will have to spend time and money on a new design (1). • Any other valid suggestion.	4	*Points marking approach.* *Up to four marks for valid justification.*

Section B

<table>
<tr><th colspan="3">Question</th><th>Answer</th><th>Marks</th><th>Guidance</th></tr>
<tr><td>5</td><td>(a)</td><td></td><td>• Data/account information/passwords could be intercepted/hacked (1) if connected to an unsecure network (1).
• A third party could mimic a real hotspot (1) and collect data from the device (1).
• Man-in-the-middle attack (1)/a third party between the user and the internet (1).
• WPA2 weak passwords can be hacked (1).
• Any other valid suggestion.</td><td>2</td><td>Points marking approach.

One mark for correct identification plus an additional one mark for valid description.</td></tr>
<tr><td></td><td>(b)*</td><td></td><td>Indicative content:
• Check the network name with the coffee shop staff.
• Visit websites that begin with ‘https’ on every page because these sites are more secure.
• Download a virtual private network; this will create a more secure link between the device and the hotspot.
• Only connect to a secured hotspot/connect with a password.
• Check the type of Wi-Fi hotspot security.
• Choose WPA2.
• Enable firewall/block traffic.
• Do not do online banking/online shopping.
• Any other valid suggestion.</td><td>8</td><td>Levels of response marking approach.

7-8 marks Has shown a detailed level of understanding by evaluating the preventative measures that could be taken. The candidate is able to provide a clear explanation of more than one measure and the consequence of these actions. 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.

4-6 marks Has shown a good level of understanding by explaining preventative measure(s) that could be taken. Explanations may concentrate on either the measure or the consequence with limited depth in the expansions. Some examples used to support explanation may not be relevant and may at times detract from</td></tr>
</table>

Question			Answer	Marks	Guidance
					fluency of narrative. *There is a line of reasoning presented with some structure. The information presented is in the most-part relevant and supported by some evidence.* *1-3 marks* Has identified points relevant to preventative measures. Limited use of examples to accompany description and ideas will be poorly expressed. *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*
6	**(a)**		• It is an example of a hoax email (1) • It is a phishing email (1)	1	*For one mark:*
6	**(b)**		• Asking for password (1) • Asking for personal details (1) • Instructing the recipient to click on the link (1) • Instructing the recipient to open the attachment (1)	3	*Points marking.* *One mark for each correct identification up to a maximum of three identifications.*

<table>
<tr><th colspan="3">Question</th><th>Answer</th><th>Marks</th><th>Guidance</th></tr>
<tr><td>6</td><td>(c)</td><td></td><td>Indicative content:
• The sender’s intentions could be to obtain personal data
• Financial loss
• Password to other accounts
• Identity theft
• Malicious intention
• Find location
• Reduce confidence in using technology
• Any other valid suggestion.</td><td>6</td><td>Levels of response marking approach.

<table><tr><td>5-6 marks</td><td>Has evaluated the impact on family member and given two or more examples.</td></tr><tr><td>3-4 marks</td><td>Has described possible impacts on family member and given at least one example or has explained possible impacts on family member and given no examples.</td></tr><tr><td>1-2 marks</td><td>Has identified possible impacts on family member. May be no example.</td></tr><tr><td>0 marks</td><td>Nothing worth of credit.</td></tr></table></td></tr>
</table>