

Modified Enlarged 24pt
OXFORD CAMBRIDGE AND RSA
EXAMINATIONS

Monday 18 January 2021 – Morning

Level 3 Cambridge Technical in IT

05839/05840/05841/05842/05877

Unit 3: Cyber security

**Time allowed: 1 hour plus your additional
time allowance**

You must have:
a clean copy of the Pre-release
(with this document)

Please write clearly in black ink.

**Centre
number**

--	--	--	--	--

**Candidate
number**

--	--	--	--

First name(s) _____

Last name _____

**Date of
birth**

D	D	M	M	Y	Y	Y	Y
---	---	---	---	---	---	---	---

READ INSTRUCTIONS OVERLEAF

INSTRUCTIONS

Use black ink.

Write your answer to each question in the space provided. You can use extra paper if you need to, but you must clearly show your candidate number, the centre number and the question numbers.

Answer ALL the questions.

Use the Insert to answer Questions 1, 2 and 3.

INFORMATION

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 (*).

ADVICE

Read each question carefully before you start your answer.

SECTION A

Answer ALL the questions.

- 1 (a) Stevenson Research has appointed a Director of Cyber Security. One of their responsibilities is to produce policies and procedures to protect the organisational data.**
- (i) Explain TWO reasons why it is important to protect the organisational data at Stevenson Research. [4]**

1

2

(ii) Identify TWO other types of data that need to be protected at Stevenson Research.

1

2

[2]

(b) Two of the cyber security threats to the data at Stevenson Research are environmental and physical.

Describe, using examples, what is meant by environmental and physical threats.

Environmental _____

Physical _____

(c) The Director of Cyber Security needs to be aware of the types, characteristics and motivations of attackers who might be a threat to Stevenson Research.

(i) Describe the following types of attacker.

Hacktivist _____

Cyber terrorist _____

[4]

7

(ii) Identify TWO characteristics of a script kiddie.

1 _____

2 _____

[2]

(iii) Describe TWO motivations of an insider.

1 _____

2 _____

[4]

2* Discuss the operational impacts of a cyber security incident on Stevenson Research. [7]

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

3 (a)* One of the tasks the Director of Cyber Security has been given is risk management. One of the ways to mitigate risks is to test for potential vulnerabilities.

Justify the use of testing for potential vulnerabilities as a method of mitigating risk. [10]

(b) The Director of Cyber Security is investigating the use of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). Describe two differences between IDS and IPS.

1

2

[4]

SECTION B

Answer ALL the questions.

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

TechnoBabble are security consultants who can be hired to consult on all areas of cyber security.

4 Three types of security incident are given below with one word missing from each. Complete the sentences below using the most appropriate word. [3]

1 _____ access includes hacking and escalation of privileges.

2 _____ includes using malware and deliberate erasure.

3 Inaccessible _____ includes account lockout and denial of service.

- 5 (a) One of the services offered is vulnerability testing. One type of vulnerability testing is penetration testing.**

Describe what is meant by penetration testing.

[2]

- (b) Identify TWO other types of vulnerability testing that could be offered by TechnoBabble.**

1

2

[2]

6 TechnoBabble has been asked to investigate a cyber security incident on a network and produce a cyber security incident report.

(a) TechnoBabble needs to categorise the incident.

Draw a line opposite to connect each incident category with its description. [4]

Incident Category	Description
Minor	Little or no impact on the system or users
Critical	Can be handled internally by IT support and security staff
Negligible	Involves a serious breach of network security
Significant	Impacts a small number of users and likely to disrupt non-essential services

(b) TechnoBabble recommends that a set of written procedures should be followed in the event of a cyber security incident.

Explain why it is an advantage to have the procedures written down.

(c) Explain TWO reasons why it is necessary to include the techniques used by the attackers to gain access to the network, in the cyber security incident report.

1 _____

2 _____

[4]

END OF QUESTION PAPER



Oxford Cambridge and RSA

Copyright Information:

OCR is committed to seeking permission to reproduce all third-party content that it uses in its assessment materials. OCR has attempted to identify and contact all copyright holders whose work is used in this paper. To avoid the issue of disclosure of answer-related information to candidates, all copyright acknowledgements are reproduced in the OCR Copyright Acknowledgements Booklet. This is produced for each series of examinations and is freely available to download from our public website (www.ocr.org.uk) after the live examination series.

If OCR has unwittingly failed to correctly acknowledge or clear any third-party content in this assessment material OCR will be happy to correct its mistake at the earliest possible opportunity.

For queries or further information please contact the Copyright Team, OCR (Oxford Cambridge and RSA Examinations), The Triangle Building, Shaftesbury Road, Cambridge CB2 8EA.

OCR is part of the Cambridge Assessment Group. Cambridge Assessment is the brand name of University of Cambridge Local Examinations Syndicate (UCLES), which is itself a department of the University of Cambridge.