OCR
Oxford Cambridge and RSA

Thursday 25 May 2023 – Afternoon

Level 3 Cambridge Technical in IT

05839/05840/05841/05842/05877 Unit 3: Cyber security

Time allowed: 1 hour
C384/2306

C384/2306

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

05839-03

Please write clearly in black ink. **Do not write in the barcodes.**

Centre number | | | | | | Candidate number | | | | |

First name(s) _____

Last name _____

Date of birth | D | D | M | M | Y | Y | Y | Y |

INSTRUCTIONS
- Use black ink.
- Write your answer to each question in the space provided. If you need extra space use the lined pages at the end of this booklet. The question numbers must be clearly shown.
- Answer **all** the questions.
- Use the Insert to answer the questions in Section A.

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 (*).
- This document has **12** pages.

ADVICE
- Read each question carefully before you start your answer.

Section A

Use the case study on **Pen Perimeter** in the **Insert** to answer the questions in this section.

Pen Perimeter has a variety of clients from different organisations.

1 **(a)** Pen Perimeter has been hired by a government department to report on the security of the data it stores.

(i) Describe **one** type of state's data that needs to be **protected**.

.....

.....

.....

..... **[2]**

(ii) Identify **one other** type of state's data that needs to be **protected**.

.....

..... **[1]**

(b) One of Pen Perimeter's clients is a healthcare provider.

Identify **two** reasons why an organisation, such as a healthcare provider, might be a **target** for a cyber security threat.

Reason 1 .....

.....

Reason 2 .....

.....

[2]

2 Pen Perimeter carried out tests for a charity.

A Test Report was created which included recommendations for improvements for the charity's cyber security.

(a) (i) Identify **three different physical** based cyber security controls that Pen Perimeter would have tested.

Control 1 .....

.....

Control 2 .....

.....

Control 3 .....

.....

[3]

(ii) Identify **two different software** based cyber security controls that Pen Perimeter would have tested.

Control 1 .....

.....

Control 2 .....

.....

[2]

(b)* Using examples, explain how the cost of implementing the recommendations of the report could **outweigh** the benefits.

.... **[7]**

(c)* Discuss the implications for **stakeholders** of the charity if they did **not** act on the recommendations of the report.

.... **[10]**

3 Pen Perimeter has been hired by a financial business to carry out a simulated cyber security attack on their network.

(a) After containing the incident, the financial business needs to **eradicate** it.

Identify **two** ways the incident could be **eradicated**.

Way 1 .....

.....

Way 2 .....

.....

[2]

The financial business uses the attack to practise its production of a cyber security incident report.

(b) (i) Why is it important to understand if the **target** of the incident was a particular department or individual?

.....

.....

.....

..... **[2]**

(ii) The incident is given a category.

Draw a line to match **each** incident category to the correct definition.

Critical	Inconvenient, loss of efficiency but able to provide services.
Minor	Loss of reputation, disruption to services, financial loss.
Significant	Organisation is no longer able to provide some critical services to users, lives may be lost.
	Minimal impact on systems, services and users.

[3]

(iii) Describe **two different** ways the capability of the attackers could be **established**.

Way 1 .....

.....

.....

.....

Way 2 .....

.....

.....

.....

[4]

(c) After the incident the financial business **updates** its documentation.

Identify **two different** items of documentation it would **update** to assist in future cyber security attacks.

Item 1 .....

.....

Item 2 .....

.....

[2]

Section B

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

4 (a) (i) What does **confidentiality** of information mean?

.....

..... **[1]**

(ii) Identify **two** measures that can be implemented to ensure the **confidentiality** of information.

Measure 1 .....

.....

Measure 2 .....

.....

[2]

(b) (i) What does **integrity** of information mean?

.....

..... **[1]**

(ii) Identify **two** measures that can be implemented to ensure the **integrity** of information.

Measure 1 .....

.....

Measure 2 .....

.....

[2]

5 **(a)** Identify **two** motivations of a cyber-criminal.

Motivation 1 .....

.....

Motivation 2 .....

.....

[2]

(b) For each cyber security incident, identify the **type** of **attacker** who would most likely be involved.

Cyber Security Incident	Type of Attacker
Changing grades in a school	
Employee releasing customer information to a rival firm	
Hacking a company and releasing information on salary gender imbalance	

[3]

(c) One of the targets for cyber security incidents is **information**.

Explain how a hacker could use **information** about an individual obtained from a cyber security incident.

.....

.....

.....

.....

.....

..... **[3]**

6 **(a)** Explain how **encryption** can be used to protect data.

.....

.....

.....

.....

.....

..... **[3]**

(b) Describe characteristics of **physical** cyber security controls that make them suitable for preventing cyber security incidents.

.....

.....

.....

.....

.....

..... **[3]**

END OF QUESTION PAPER

ADDITIONAL ANSWER SPACE

If additional answer space is required, you should use the following lined pages. The question numbers must be clearly shown in the margins – for example, 2(b) or 3(a).