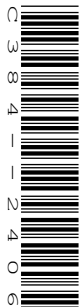# OCR
Oxford Cambridge and RSA

Thursday 23 May 2024 – Afternoon

Level 3 Cambridge Technical in IT

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

Time allowed: 1 hour

C384/2406

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

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

Centre number ☐☐☐☐☐   Candidate number ☐☐☐☐

First name(s) _____

Last name _____

Date of birth ☐☐ ☐☐ ☐☐☐☐

INSTRUCTIONS
- Use black ink.
- Write your answer to each question in the space provided. If you need extra space use the lined page 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 **Charlie's Home Network** in the **Insert** to answer the questions in this section.

1

(a) One of the aims of cyber security is to protect information by making sure information has confidentiality, integrity and availability.

(i) Describe **availability** of information.

....

....

....

.... **[2]**

(ii) Give **one** example of a **cyber security measure** Charlie can use to protect the availability of their information.

....

.... **[1]**

(b) One of the threats to cyber security is environmental.

Identify one **environmental** threat and describe how Charlie's network is vulnerable to it.

Environmental threat ....

....

Description ....

....

[2]

2
(a) Charlie suspects the teenager who lives on the other side of the street has hacked into their network.

One motivation for the teenager is thrill seeking.

Identify **two other** motivations for the teenager to hack into Charlie's home network.

Motivation 1 ....

....

Motivation 2 ....

....
[2]

(b) After doing some research, Charlie believes that the teenager is a script kiddie.

One characteristic of a script kiddie is that they are likely to be a teenager.

Identify **two other** characteristics of a script kiddie.

Characteristic 1 ....

....

Characteristic 2 ....

....
[2]

(c) Identify **two other** types of attacker who might have hacked into Charlie's network.

1 ....

....

2 ....

....
[2]

Turn over

3

(a) Following the hack on their network, Charlie discovers that some files cannot be opened.

(i) Identify and describe the **type of cyber security incident** that has occurred.

Type of incident ....

....

Description ....

....

[2]

(ii) Charlie has found some of their personal information posted to a local neighbourhood website.

Identify and describe the **type of cyber security incident** that has occurred.

Type of incident ....

....

Description ....

....

[2]

(b) The disruption to Charlie's life caused by the attack on their network includes loss of privacy, financial and reputational damage.

Explain **two other** ways Charlie's life could have been **disrupted** by the attack on their network.

Way 1 ....

....

....

....

....

Way 2 ....

....

....

....

....

[6]

4

(a)* The ethical impacts on Charlie of being attacked include loss of privacy, financial and reputational damage.

Discuss the **ethical impacts** of loss of privacy, financial and reputational damage on Charlie.

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

.... **[7]**

(b) Charlie decides to take an online course in cyber security.

One of the modules is about vulnerability testing.

Describe the following vulnerability testing techniques.

Penetration testing ....

....

....

....

....

....

Sandboxing ....

....

....

....

....

[4]

(c) Explain why fuzzing would **not** be an appropriate vulnerability technique for Charlie to use on their network.

....

....

....

....

....

.... **[2]**

Turn over

(d) Explain **three** ways Charlie can mitigate the risk of a future attack on their network.

1 ....

....

....

....

2 ....

....

....

....

3 ....

....

....

....

[6]

Section B

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

A company has implemented a set of procedures to improve the security of its network and started to use cryptography to protect valuable documents.

When starting work on a Monday morning, the company was surprised to discover that it had been the victim of a ransomware attack.

5
(a) Explain why the company's reliance on **procedures and cryptography** has led to an incorrect view that its systems were safe.

....

....

....

....

....

....

....

....

....

....

....

.... **[6]**

(b) Describe **two** actions the company could take to **eradicate the incident**.

Action 1 ....

....

....

....

Action 2 ....

....

....

....

[4]

Turn over

(c)* The company is completing a Cyber Security Incident Report (CSIR).

One of the sections relates to the **impact of the incident on business, data and recovery time**.

Explain how this section of the CSIR would be used by the company.

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

.... **[10]**

END OF QUESTION PAPER

EXTRA ANSWER SPACE

If you need extra space use this lined page. You must write the question numbers clearly in the margin.

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....