OCR
Oxford Cambridge and RSA

Wednesday 16 January 2019 – Morning

LEVEL 3 CAMBRIDGE TECHNICAL IN IT

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

Duration: 1 hour

C384/1901

You must have:
- a clean copy of the pre-release (Insert C387)

First Name		Last Name	
Centre Number		Candidate Number	
Date of Birth	D D M M Y Y Y Y		

INSTRUCTIONS
- Use black ink.
- Complete the boxes above with your name, centre number, candidate number and date of birth.
- Answer **all** the questions.
- Write your answer to each question in the space provided.
- If additional answer space is required, you should use the lined page(s) at the end of this booklet. The question number(s) must be clearly shown.

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 the question marked with an asterisk (*).
- This document consists of **12** pages.

FOR EXAMINER USE ONLY	
Question No	**Mark**
1	/28
2	/12
3	/6
4	/11
5	/3
Total	**/60**

C384/1901/3

OCR is an exempt Charity

Turn over

Answer **all** the questions.

Section A

This section relates to the case study about a cyber security attack on a customer in Nepal.

1 Whilst on holiday in Kathmandu, Mr Thapa used a Wi-Fi access point in a coffee shop to connect his personal mobile phone to the internet to perform a number of tasks. Whilst connected his phone was hacked.

(a) The diagram below shows three types of attacker and three definitions.

Draw a line to connect each type of attacker to its correct definition.

Type of attacker		Definition

hactivist		individual who often sends an email trying to get you to pay for goods or opportunities without there being any real end product
phisher		individual who tries to obtain financial or confidential information by sending an email that looks like it has come from a legitimate organisation
scammer		individual who uses computers to promote their own views on a particular issue

[3]

(b) Explain **one** reason why Mr Thapa would want to keep his phone secure.

....

....

....

....**[2]**

(c) One type of attacker is a script kiddie. Complete the table below to identify the likely characteristics of a script kiddie.

Characteristic	Script kiddie
age	....
location	....
social group	....

[3]

(d) Discuss the reasons why people, such as Mr. Thapa, can be targets of cyber security attacks in a coffee shop environment.

[7]

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

Turn over

....

....

....

....

....

(e) Identify and describe **one** method that could be used by attackers to access Mr Thapa's phone.

....

....

....

....

....

....**[3]**

Following the phone hack, personal information has been extracted from Mr Thapa's phone by the attacker.

(f) Using examples, describe **three different** ways Mr Thapa's life could be disrupted by cyber criminals using the information obtained from the phone hack.

1...

....

....

....

2...

....

....

....

3...

....

....

....

[6]

(g) Describe **two different** access controls Mr Thapa could implement to secure his phone.

1..

....

....

....

2..

....

....

....

[4]

The franchise that owns the coffee shop has employed a cyber security team to investigate the hack into Mr Thapa's phone.

2   (a) Identify **three** pieces of information Mr Thapa needs to provide to the cyber security team in order for them to create a cyber security incident report. For **each** piece of information, state why it is needed by the cyber security team.

1..

....

Why needed ....

....

2..

....

Why needed ....

....

3..

....

Why needed ....

....

[6]

Turn over

(b) Mr Thapa has been asked to cooperate with the cyber security team during its investigation.

Explain why it is important to Mr Thapa that each member of the cyber security team has a different role.

....

....

....

....**[2]**

(c) Explain **two** ways that the coffee shop could use the review of the incident created by the cyber security team.

1..

....

....

....

2..

....

....

....

[4]

Section B

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

3   Describe, using an example, how cyber security aims to protect the confidentiality, integrity and availability of data.

Confidentiality ....

....

....

....

Integrity ....

....

....

....

Availability ....

....

....

....

[6]

4   **(a)*** Justify the effectiveness of using network intrusion detection systems (NIDS) to protect the information stored on a server.

[10]

....

....

....

....

....

....

....

....

....

....

....

....

Turn over

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

(b) Identify **one other** type of intrusion detection system that could be used.

....**[1]**

5 A company should regularly undertake cyber security risk management.

Explain why it is not possible to remove all risk.

....

....

....

....

....

....**[3]**

END OF QUESTION PAPER

9

ADDITIONAL ANSWER SPACE

If additional answer space is required, you should use the following lined page(s). The question number(s) must be clearly shown in the margin(s) – for example 1(d) or 4(a).

© OCR 2019

OCR

Oxford Cambridge and RSA

C384/1901