

CAMBRIDGE TECHNICALS LEVEL 3 (2016)

Examiners' report

IT

05838–05842, 05877

Unit 3 January 2023 series

Contents

Introduction3

Unit 3 series overview4

Section A overview5

 Question 1 (a)5

 Question 1 (b) (i)5

 Question 1 (b) (ii)6

 Question 1 (b) (iii)6

 Question 1 (c)7

 Question 1 (d)8

 Question 1 (e)8

 Question 1 (f)*9

 Question 2 (a)*10

 Question 2 (b)11

 Question 2 (c)11

Section B overview13

 Question 3 (i)13

 Question 3 (ii)13

 Question 4 (i)14

 Question 4 (ii)15

 Question 4 (iii)16

 Question 517

Introduction

Our examiners' reports are produced to offer constructive feedback on candidates' performance in the examinations. They provide useful guidance for future candidates.

The reports will include a general commentary on candidates' performance, identify technical aspects examined in the questions and highlight good performance and where performance could be improved. The reports will also explain aspects which caused difficulty and why the difficulties arose, whether through a lack of knowledge, poor examination technique, or any other identifiable and explainable reason.

Where overall performance on a question/question part was considered good, with no particular areas to highlight, these questions have not been included in the report.

A full copy of the question paper and the mark scheme can be downloaded from OCR.

Would you prefer a Word version?

Did you know that you can save this PDF as a Word file using Acrobat Professional?

Simply click on **File > Export to** and select **Microsoft Word**

(If you have opened this PDF in your browser you will need to save it first. Simply right click anywhere on the page and select **Save as . . .** to save the PDF. Then open the PDF in Acrobat Professional.)

If you do not have access to Acrobat Professional there are a number of **free** applications available that will also convert PDF to Word (search for PDF to Word converter).

Unit 3 series overview

This unit is mandatory for the Extended Certificate, Diploma and Extended Diploma and optional for all pathways for the Introductory Diploma and Foundation Diploma.

The unit focuses on:

- an understanding of cyber security and the issues surrounding it
- measures that can be used to protect against cyber security incidents
- an understanding of how to manage cyber security incidents.

The paper is divided into two Sections – A and B. Section A is worth 60% (40 marks) and are based around a pre-release scenario. The pre-release contains areas for further research that the candidate is expected to undertake, and which form the basis of the questions to be asked. Section B is worth 40% (20 marks) and each question has its own short scenario.

Candidates who did well on this paper generally did the following:	Candidates who did less well on this paper generally did the following:
<ul style="list-style-type: none"> • used technical terms • related their responses to the scenario in the question • used the keywords in the question to give appropriate depth to their response. 	<ul style="list-style-type: none"> • answered the question they thought was being asked, not the one actually being asked • repeating the same point several times in different ways • giving a response that has been eliminated in the question.

Many candidates did not attempt all questions. This prevents them from gaining marks and therefore potentially accessing the higher grades.

We would recommend attempting answers to all questions, as candidates may gain some marks from their response, even if they do not manage to complete the question in full.

Candidates need to learn the key words in the specification and their associated definitions and then apply them to the scenario.

There is evidence that candidates are not familiar with the technical terms used in cyber security.

Section A overview

The pre-release identifies key research topics that the candidates should have spent some time working on. They need to have cross referenced the topics against the specification and identified keywords that will assist them in linking the research topics to the questions asked. Responses should be given in the context of the case study in the pre-release.

Question 1 (a)

- 1 (a) Mia has been told that she needs to protect the personal data submitted by the members on her network from both information disclosure and data modification.

Describe the difference between information disclosure and data modification.

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

Candidates responded very well to this question with the majority scoring highly, achieving both marks.

Question 1 (b) (i)

- (b) One of the types of security incident that Mia needs to be aware of, is **denial of service (DoS)**.

(i) What does **denial of service (DoS)** mean?

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

Candidates responded very well to this question with the majority scoring highly. Those that did not tended to describe how a DoS attack would take place.

Question 1 (b) (ii)

(ii) Identify **two** ways Mia can **prevent** a DoS attack.

1

.....

2

.....

[2]

Many of the methods that candidates identified would not prevent a DoS attack. This demonstrated a lack of knowledge of how a DoS attack works and what can be used to stop it or deflect it. There were many responses related to anti-virus and passwords.

Question 1 (b) (iii)

(iii) Identify **one other** type of cyber security incident Mia would need to protect against.

.....

..... [1]

It was disappointing to see many responses replicate technical terms from the paper. This is a learnt response that directly links to a specification point and one of the tasks in the pre-release.

Misconception



Social engineering is not a type of cyber security incident. It is an overarching term that leads to data theft, hacking, unauthorised access and so on. These are the incidents, social engineering is the vehicle that leads to them.

Question 1 (c)

(c) Mia has been warned that she might receive emails from scammers.

Describe **two** motivations of a scammer who sends emails to Mia.

1

.....

.....

.....

2

.....

.....

.....

[4]

Many candidates achieved the first mark – the identification of the motivation – with financial being the most common one. However, candidates did not give an adequate description and very few related it to the context and to Mia and/or the club.

Question 1 (d)

(d) There are different types of attacker who may target Mia and the data on her network.
Draw a line to connect each type of attacker with their description.

One has been done for you.

Type of Attacker	Description
Insider	An attacker who attempts to discover exploits and sells them
Phisher	An attack on a network or computer system by a person with authorised access
Hactivist	An attacker who tries to get individuals to reveal personal information by sending emails pretending to be from companies
Vulnerability Broker	An attack on a network or computer system to achieve social or political goals

[3]

This was very well answered with most candidates gaining full marks.

Question 1 (e)

(e) One of the targets is the **health data** entered by members.
Describe how a cyber criminal could use the **health data** they targeted.

.....

.....

.....

..... [2]

The focus of the response from the candidates needed to be on the health data. Many responses were generic. Those that did relate their answer to the scenario gave good responses.

Question 1 (f)*

(f)* Discuss the impact on Mia, in her role as Membership and Web Officer, if an attacker gained access to the webserver.

[10]

.....

.....

.....

.....

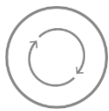
.....

.....

This question was not answered well. Many candidates described the actions that Mia would need to take once she had discovered the attack. Very few focused on the impact of the attack on her role. There was also a misconception that Mia was the owner of the running club and that as such she would be personally responsible.

Those that did make points regarding the impact on Mia did not expand and explain the points made. Many of the responses were a string of identifications rather than the in-depth explanation that an essay requires at this level.

Assessment for learning



Essay questions are marked using bands and not using points. This means that the candidate needs to be making a few points, but each point needs to show the depth of their knowledge and understanding rather than many points which demonstrate a superficial breadth.

Each point requires an explanation, backed up with examples relevant to the question. The explanation needs to make up most of the response rather than be added as an afterthought.

Misconception



Candidates frequently confused an IDS and an IPS. One detects and the other prevents. It is important that within the context of the question the correct one is given.

Section B overview

This section is not based on the pre-release material. Each question is given a short context and candidates are expected to use it, where appropriate, within their responses.

Question 3 (i)

3 (i) Identify **one** UK law that applies to IT.

.....

..... [1]

The majority of candidates achieved this mark.

Question 3 (ii)

(ii) Describe the impact of the law you have identified on an organisation.

.....

.....

.....

.....

.....

..... [3]

Candidates who gave the DPA in (i) did much better in this part than those that selected any other UK law. An understanding of the principles allowed them to achieve all the marks.

Assessment for learning



Where the question is linked – the second part is dependent on the first, it is important to read the whole question before giving a response. There will be some responses that, whilst correct for the first part, do make achieving all the marks for the second part difficult.

Question 4 (i)

4 A company has suffered a cyber security incident and an incident report needs to be completed.

(i) Describe why it is necessary to record the date of the incident in the report.

.....

.....

.....

..... [2]

This question was poorly answered. Many linked the date of the event to being able to find it again or to identify it. The date is not appropriate for either of these and so did not achieve marks.

Question 4 (ii)

(ii) The cyber security incident can be placed into one of four categories.

Complete the paragraph describing the different categories.

Use the following list of terms.

You do not need to use all the words.

- critical
- effect
- impact
- insignificant
- major
- minor
- serious
- significant
- small
- substantial

If the incident is categorised as _____ then this means it involves a serious breach of network security. A negligible incident is one that has little or no _____ on the system or the users. A _____ incident is likely to disrupt non-essential services. A _____ incident can be handled internally by IT support.

[4]

This was generally answered well with most candidates achieving 2 marks. Many of the terms given in the list were not those associated with the categories and it is important that candidates are aware of the technical terminology associated with cyber security.

Question 4 (iii)

(iii) One of the sections of the **cyber security incident** report is responses needed.

Identify **two** different groups of people who would need to be informed of the **cyber security incident**.

For each group, explain why they would need to know.

Group:

Explanation:

.....

.....

.....

Group:

Explanation:

.....


.....

.....

[6]

When completing the cyber security incident report, the IT team would already be aware of the attack. This section within the report is those groups who would be needed to be informed once the initial plan has been put into place. The most common correct responses focused on the government and those who had been hacked. In many responses however the explanation as to why they needed to be informed was weak or missing with the focus being on a description of the group.

Misconception

 Under the DPA 2018, if a data breach has occurred there is not an absolute requirement to notify the individual that their account has been hacked.

Supporting you

Reviews of marking

If any of your students' results are not as expected, you may wish to consider one of our post-results services. For full information about the options available visit the [OCR website](#).

Keep up-to-date

We send a monthly bulletin to tell you about important updates. You can also sign up for your subject specific updates. If you haven't already, [sign up here](#).

OCR Professional Development

Attend one of our popular CPD courses to hear directly from a senior assessor or drop in to a Q&A session. Most of our courses are delivered live via an online platform, so you can attend from any location.

Please find details for all our courses on the relevant subject page on our [website](#) or visit [OCR professional development](#).

Signed up for ExamBuilder?

ExamBuilder is the question builder platform for a range of our GCSE, A Level, Cambridge Nationals and Cambridge Technicals qualifications. [Find out more](#).

ExamBuilder is **free for all OCR centres** with an Interchange account and gives you unlimited users per centre. We need an [Interchange](#) username to validate the identity of your centre's first user account for ExamBuilder.

If you do not have an Interchange account please contact your centre administrator (usually the Exams Officer) to request a username, or nominate an existing Interchange user in your department.

Need to get in touch?

If you ever have any questions about OCR qualifications or services (including administration, logistics and teaching) please feel free to get in touch with our customer support centre.

Call us on
01223 553998

Alternatively, you can email us on
support@ocr.org.uk

For more information visit

 **ocr.org.uk/qualifications/resource-finder**

 **ocr.org.uk**

 **facebook.com/ocrexams**

 **twitter.com/ocrexams**

 **instagram.com/ocrexaminations**

 **linkedin.com/company/ocr**

 **youtube.com/ocrexams**

We really value your feedback

Click to send us an autogenerated email about this resource. Add comments if you want to. Let us know how we can improve this resource or what else you need. Your email address will not be used or shared for any marketing purposes.



I like this



I dislike this

Please note – web links are correct at date of publication but other websites may change over time. If you have any problems with a link you may want to navigate to that organisation's website for a direct search.



OCR is part of Cambridge University Press & Assessment, a department of the University of Cambridge.

For staff training purposes and as part of our quality assurance programme your call may be recorded or monitored. © OCR 2023 Oxford Cambridge and RSA Examinations is a Company Limited by Guarantee. Registered in England. Registered office The Triangle Building, Shaftesbury Road, Cambridge, CB2 8EA. Registered company number 3484466. OCR is an exempt charity.

OCR operates academic and vocational qualifications regulated by Ofqual, Qualifications Wales and CCEA as listed in their qualifications registers including A Levels, GCSEs, Cambridge Technicals and Cambridge Nationals.

OCR provides resources to help you deliver our qualifications. These resources do not represent any particular teaching method we expect you to use. We update our resources regularly and aim to make sure content is accurate but please check the OCR website so that you have the most up to date version. OCR cannot be held responsible for any errors or omissions in these resources.

Though we make every effort to check our resources, there may be contradictions between published support and the specification, so it is important that you always use information in the latest specification. We indicate any specification changes within the document itself, change the version number and provide a summary of the changes. If you do notice a discrepancy between the specification and a resource, please [contact us](#).

You can copy and distribute this resource freely if you keep the OCR logo and this small print intact and you acknowledge OCR as the originator of the resource.

OCR acknowledges the use of the following content: N/A

Whether you already offer OCR qualifications, are new to OCR or are thinking about switching, you can request more information using our [Expression of Interest form](#).

Please [get in touch](#) if you want to discuss the accessibility of resources we offer to support you in delivering our qualifications.