OCR
Oxford Cambridge and RSA

CAMBRIDGE TECHNICALS LEVEL 3 (2016)

Examiners' report

IT

05838–05842, 05877, 05885, 05886

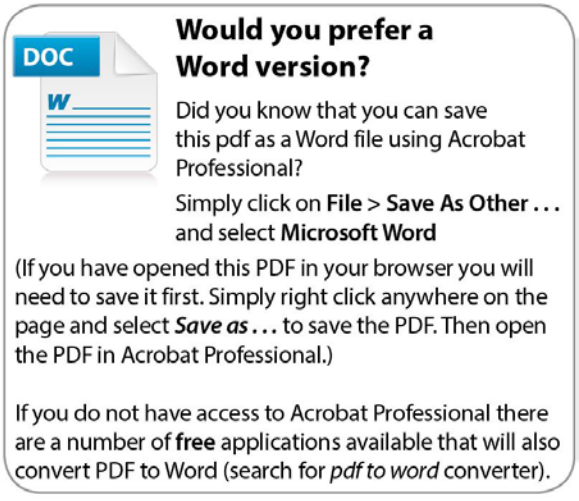
Cambridge TECHNICALS

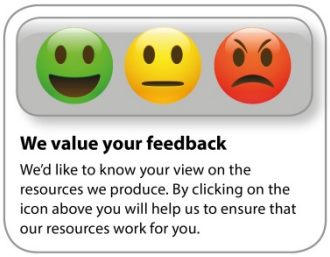
Unit 3 Summer 2019 series

Version 1

Contents

Introduction 3
Paper Unit 3 series overview 4
Question 1 (a) 5
Question 1 (b) 5
Question 1 (c) 7
Question 1 (d) 8
Question 1 (e) 8
Question 2 9
Question 3 (a) 9
Question 3 (b) 10
Question 4 (a) 10
Question 4 (b) 11
Question 5 11
Question 6 12
Copyright information 12





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 can be downloaded from OCR.

Paper Unit 3 series overview

Candidates' performance for this series was in line with that seen in previous series. Some candidates seemed extremely well prepared for the examination, and gave clear and concise answers, especially for Section A.

Section A is based solely on the context given by the pre-examination tasks. It was clear that some candidates had prepared themselves very well for the examination and had explored the pre-examination tasks in some depth. However, other candidates gave the impression that they had done minimal preparation for the examination and gave answers that were extremely generalised.

Section B is a general section with each question based on individual scenarios. The focus of this section is therefore on a wider understanding of the syllabus. Performance was mixed here. Some candidates had a clear understanding of the wider syllabus, whilst others struggled with this section.

Question 1 (a)

1 The cyber security department of Progressive Moniez has been contacted after the company was the victim of an attack. The first step is to complete a cyber security incident report.

(a) Describe the purpose of a cyber security incident report.

.....

.....

.....

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

This question was answered well by the majority of candidates.

Question 1 (b)

(b) Use the template below to complete the cyber security incident report for the attack committed against Progressive Moniez in January 2019. Part of it has already been completed.

Cyber Security Incident Report	
Title	**[1]**
Date	*January 18th 2019*
Target	**[1]**
Type of Incident(s)	**[1]**
Description of Incident	*Funds were taken from one of the cryptocurrencies stored and customer details were also accessed.*
Type of attacker(s)	**[1]**
Purpose of Incident(s)	**[2]**
Techniques used by attacker(s)	**[2]**
Impact on the business	**[2]**

Overall, candidates seemed fairly well prepared for this question, although some were caught out by aspects. It is important to remember that the Cyber Security Incident Report was created internally, therefore.

For the title, candidates needed to give a title that would differentiate the report from others. As it was an internal report, there was no need to state the name of the organisation. Titles such as "cyber security incident" were too vague, as they did not differentiate.

For the target, there was a wide range of answers given whereas, in reality, the targets were customer data and private keys. This part of the question proved a challenge for candidates.

For the type of incident, candidates were generally more successful than in other items on the report. Typically, candidates stated that was either unauthorised access or a data loss.

For type of attacker, many candidates identified "script kiddie" or "insider", with others going for Cyber Criminal. However, other candidates opted for "hacker". It is unlikely that such a generic term would be acceptable as an answer for this paper, as candidates are expected to have learnt about the characteristics of the different types of attacker.

Some candidates suggested that a vulnerability broker may have been responsible for the attack. A vulnerability broker is considered to be a trader in known vulnerabilities, rather than someone who identifies or exploits them, and so this was not accepted.

Successful answer to the **Purpose of the incident** question mainly focused on attempts to gain access to cyber currency. This attempt was based on an initial attack on customer data, and so candidates had to be clear between the relationship between these two targets for full marks to have been given for this aspect.

For **techniques used by attackers,** candidates were expected to state two methods. The scenario included some very clear points and many candidates picked these up. Typically, candidates gave "third party code" and forms of social engineering as answers here.

Finally, for **impact on the business**, candidates could describe one impact, or identify two. Many candidates listed more than two answers, in which case, the first two given were considered. Overall, this part of the question was well answered, although candidates' knowledge of the GDPR regulations could be improved.

Question 1 (c)

(c) The organisation, Progressive Moniez, was one target of the attack. Identify **two other** targets of the attack for each, explain why they would have been targeted.

Target 1.....

.....

Reason .....

.....

.....

.....

Target 2.....

.....

Reason .....

.....

.....

.....

[6]

The vast majority of candidates missed the point of this question. The focus was on other targets who were targeted as part of the main attack on Progressive Moniez. Candidates took this as a question about other entities who could have been targeted **at the same** time, rather than as part of the same attack. Similar questions to this have been asked in the past, with similar outcomes. The whole of Question 1 is about a single attack, and where candidates are asked to consider how others may have been targeted as part of that attack, their focus must be on how others could have been targeted **in order to improve or facilitate** the original attack.

For example, many candidates correctly identified customers as a target of the attack. However, this answer was then, typically, expanded into an answer about customers' personal details, presumably as an attack on their private finances. However, within the context of this attack, the correct answer was based on access to virtual wallets etc.

Similarly, "staff" was an acceptable target. However, again, expansions focused on attacks on staff accounts or other targets.

In both cases, the expansions would be considered separate attacks, and not part of the main attack on which the question focused.

Question 1 (d)

(d) Describe **three** features of an intrusion prevention system (IPS) that could be used by Progressive Moniez to protect its network.

Feature 1 .....

.....

.....

.....

Feature 2 .....

.....

.....

.....

Feature 3 .....

.....

.....

.....

[6]

The list of possible answers here is very long. Some candidates had a very good understanding of features of an IPS and coped with this question very well. Many gave some really good descriptions of three separate features.

Others however, appeared to have a passing knowledge, and tended to repeat their answers, or gave generic descriptions which suggested a lack of technical understanding of how an IPS operates.

Question 1 (e)

(e)* Evaluate the benefits to Progressive Moniez of using monitoring and control systems for cyber security.

.....**[7]**

In order to evaluate, candidates should be making value judgements as part of their overall answer.

This question could be answered by an evaluation of aspects of monitoring and control systems, or, as was intended, an evaluation of monitoring and control systems overall.

Few candidates gave answers that achieved beyond MB2 for this question, as very few attempted to evaluate, but focused on describing such systems. Where candidates did attempt to describe the systems, this was generally successful, although a small minority of candidates misinterpreted the question, and focused on monitoring staff.

Question 2

2* Discuss the implications of cyber security legislation on Progressive Moniez.

.....

.....**[10]**

Where candidates had a good understanding of cyber security legislation and linked their answer to the initial attack on Progressive Moniez, thereby using relevant examples, there were some really good answers to this question. Overall, this answer showed a good understanding of cyber security legislation (in contrast to Question 1b, strangely) and a good number of candidates achieved at least MB2 for this Question.

Question 3 (a)

3 (a) The diagram below shows three terms associated with cyber security and three descriptions.

Draw a line to connect each term to the correct description.

Term	Description
Confidentiality	An assurance that the information is trustworthy and accurate
Integrity	A guarantee of access to the information which is required
Availability	Protecting the information from being disclosed to unauthorised individuals

[3]

The vast majority of candidates were able to correctly link all three terms with the relevant description.

Question 3 (b)

(b) Identify the type of cyber security incident from the definition given.

Definition	Type
Making the data irretrievable	
Altering the data	
Account lockouts or denial of service	

[3]

This question proved more of a challenge than presented by question 3a. Some candidates correctly identified all three types of cyber security incident from the description, but these were the minority.

Of the majority of candidates, some attempted to repeat the description, as the type. Whilst there was, clearly, an extent to which the type of attack could be gleaned from the description, simply repeating the description was not acceptable.

Whilst the mark scheme accepted alternatives, it was noticeable that candidates tended to use the terms given in the mark scheme. Of the three, the third ("inaccessible"), proved to be the most challenging, with relatively few candidates correctly identifying this type of incident.

Question 4 (a)

4 **(a)** Daniil stores his data on a memory stick. He is concerned that if he loses the memory stick, his data could still be accessed. He has been told that he should encrypt the data on the memory stick.

Explain how encryption could be used to protect the data on the memory stick.

.....**[4]**

Section B of this paper assesses candidates' understanding of terms and concepts with fresh scenarios. Effectively, this question was asking candidates for an explanation of how encryption worked. Considering that the focus of this paper is cyber security, in which encryption plays a big role, a surprisingly small number of candidates were able to explain how encryption works in any depth. Whilst all individual answers on the mark scheme were seen, candidates rarely scored above 2 marks for this question.

Question 4 (b)

(b) Identify **one other** method that Daniil could use to protect his data.

.....

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

Candidates could provide any method of protection for this question. However, candidates had to show an understanding of the question, and therefore simply stating "store in the cloud", or, occasionally "the cloud", was insufficient.

Question 5

5 Identify and describe **two** possible motivations of a cyber attacker.

Motivation 1.....

Description.....

.....

.....

Motivation 2.....

Description.....

.....

.....

[4]

The majority of candidates scored at least 2 marks here, with a sizeable proportion achieving full marks.

Where candidates did not achieve the marks, this was usually because the answers were too vague, rather than incorrect. For example "money" is not a motivation, and neither is personal gain. Both terms are close to being correct, but candidates need to be more precise in their answer than these examples.

Question 6

6 Explain **two** reasons why a company might want to employ an ethical hacker.

Reason 1.....

.....

.....

.....

Reason 2.....

.....

.....

.....

[4]

Virtually all candidates knew what was meant by the term "ethical hacker" and of those, virtually all achieved at least one mark, with most expanding the reason with a good explanation.

However, few were able to give a second reason, with many attempting to provide the same answer twice, but in a different way.

Copyright information

Any reference to existing companies or organisations is entirely coincidental and is not intended as a depiction of those companies or organisations.

Supporting you

For further details of this qualification please visit the subject webpage.

Review of results

If any of your students' results are not as expected, you may wish to consider one of our review of results services. For full information about the options available visit the OCR website. If university places are at stake you may wish to consider priority service 2 reviews of marking which have an earlier deadline to ensure your reviews are processed in time for university applications.

Mark grade boundaries

Find the grade boundaries for this series on the OCR website.

CPD Training

Attend one of our popular CPD courses to hear exam feedback directly from a senior assessor or drop in to an online Q&A session.

Please find details for all our courses on the relevant subject page on our website.

www.ocr.org.uk

The small print

OCR Resources: *the small print*

OCR's resources are provided to support the delivery of OCR qualifications, but in no way constitute an endorsed teaching method that is required by OCR. Whilst every effort is made to ensure the accuracy of the content, OCR cannot be held responsible for any errors or omissions within these resources. We update our resources on a regular basis, so please check the OCR website to ensure you have the most up to date version.

This resource may be freely copied and distributed, as long as the OCR logo and this small print remain intact and OCR is acknowledged as the originator of this work.

Our documents are updated over time. Whilst every effort is made to check all documents, there may be contradictions between published support and the specification, therefore please use the information on the latest specification at all times. Where changes are made to specifications these will be indicated within the document, there will be a new version number indicated, and a summary of the changes. If you do notice a discrepancy between the specification and a resource please contact us at: resources.feedback@ocr.org.uk.

Whether you already offer OCR qualifications, are new to OCR, or are considering switching from your current provider/awarding organisation, you can request more information by completing the Expression of Interest form which can be found here: www.ocr.org.uk/expression-of-interest

Please get in touch if you want to discuss the accessibility of resources we offer to support delivery of our qualifications: resources.feedback@ocr.org.uk

Looking for a resource?

There is now a quick and easy search tool to help find **free** resources for your qualification:

www.ocr.org.uk/i-want-to/find-resources/

www.ocr.org.uk

OCR Customer Support Centre

Vocational qualifications

Telephone 02476 851509
Facsimile 02476 851633
Email vocational.qualifications@ocr.org.uk

OCR is part of Cambridge 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.*

Cambridge Assessment

CERTIFIED ISO 9001 UKAS MANAGEMENT SYSTEMS 001