OCR
Oxford Cambridge and RSA

Cambridge **TECHNICALS LEVEL 2**

IT

Feedback on the June 2018 on-screen test (including selected exemplar candidate answers)

Unit 2 – Essentials of cyber security

Version 1

ocr.org.uk/ict

CONTENTS

INTRODUCTION

This resource brings together the questions from the June 2018 examined unit (Unit2), the marking guidance, the examiners comments and the exemplar answers into one place for easy reference.

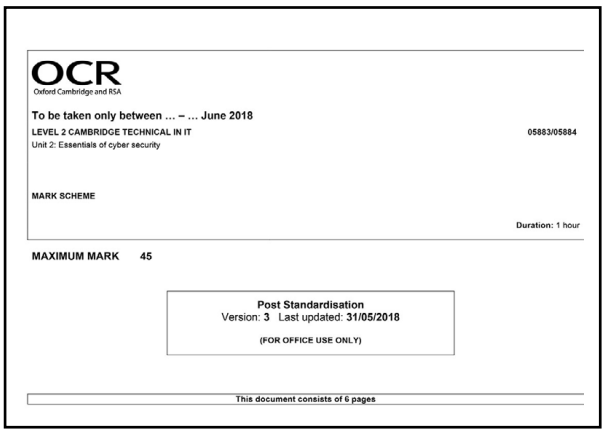
The examiner's comments are taken from the Report to Centre for this question paper. This report and the mark scheme are available from Interchange:

https://interchange.ocr.org.uk/Modules/PastPapers/Pages/PastPapers.aspx?menuindex=97&menuid=250

This on-screen test is delivered through our Surpass testing service.

Link to further information about Surpass:

http://www.ocr.org.uk/administration/stage-3-assessment/vocational-qualifications/on-screen-tests/



OCR
Oxford Cambridge and RSA

To be taken only between ... – ... June 2018
LEVEL 2 CAMBRIDGE TECHNICAL IN IT 05883/05884
Unit 2: Essentials of cyber security

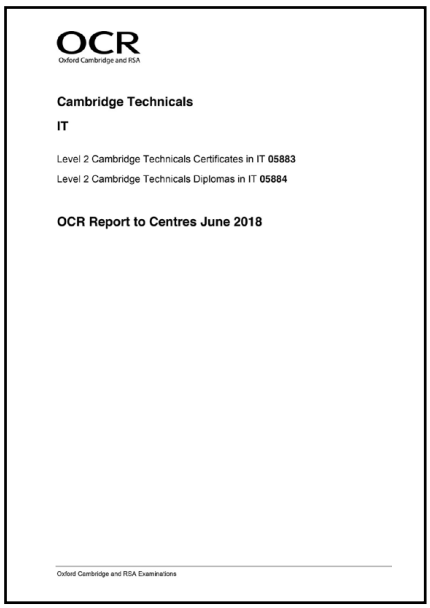
MARK SCHEME

Duration: 1 hour

MAXIMUM MARK 45

Post Standardisation
Version: 3 Last updated: 31/05/2018
(FOR OFFICE USE ONLY)

This document consists of 6 pages



OCR
Oxford Cambridge and RSA

Cambridge Technicals
IT

Level 2 Cambridge Technicals Certificates in IT 05883
Level 2 Cambridge Technicals Diplomas in IT 05884

OCR Report to Centres June 2018

Oxford Cambridge and RSA Examinations

GENERAL EXAMINER COMMENTS ON THE PAPER

Many candidates demonstrated knowledge gaps in relation to the unit content. Centres should ensure that candidates are familiar with all areas of the unit content prior to being entered for the external examination.

The correlation between content, context and command word also appeared to be limited. Candidates should be aware of the differing command words, e.g. identify, describe, explain, discuss, and the demands of each of these and how these command words require different depths of response.

Resources which might help address the examiner comments:

From the link below, you'll find 'The OCR guide to examinations' (along with many other skills guides)
http://www.ocr.org.uk/i-want-to/skills-guides/

Command verbs definitions
http://www.ocr.org.uk/Images/273311-command-verbs-definitions.pdf

Questions 1(a), (b) and (c)

View Mark Scheme | View Marking History | Add Comment | Replay

Mark: 0 / 2

(a) One target for a cyber security attack is an organisation.

Identify **two** other targets.

1 _____

2 _____

[2]

- Individuals (1)
- Equipment (1)
- Data/Information (1)

View Mark Scheme | View Marking History | Add Comment | Replay

Mark: 0 / 1

(b) Identify the type of cyber attacker who 'sends emails asking a person to click on a link to change their log-in details'.

_____

[1]

- Phisher (1)

View Mark Scheme | View Marking History | Add Comment | Replay

Mark: 0 / 2

(c) Data can be lost during a cyber security incident.

Identify **two** types of cyber security incidents where data is lost.

1 _____

2 _____

[2]

- Data destruction (1)
- Data theft (1)

Mark Scheme Guidance

Question 1(a):

Points marking approach.

Two from list.

Question 1(b):

Correct answer only.

Question 1(c):

Correct answer only.

Examiner comments

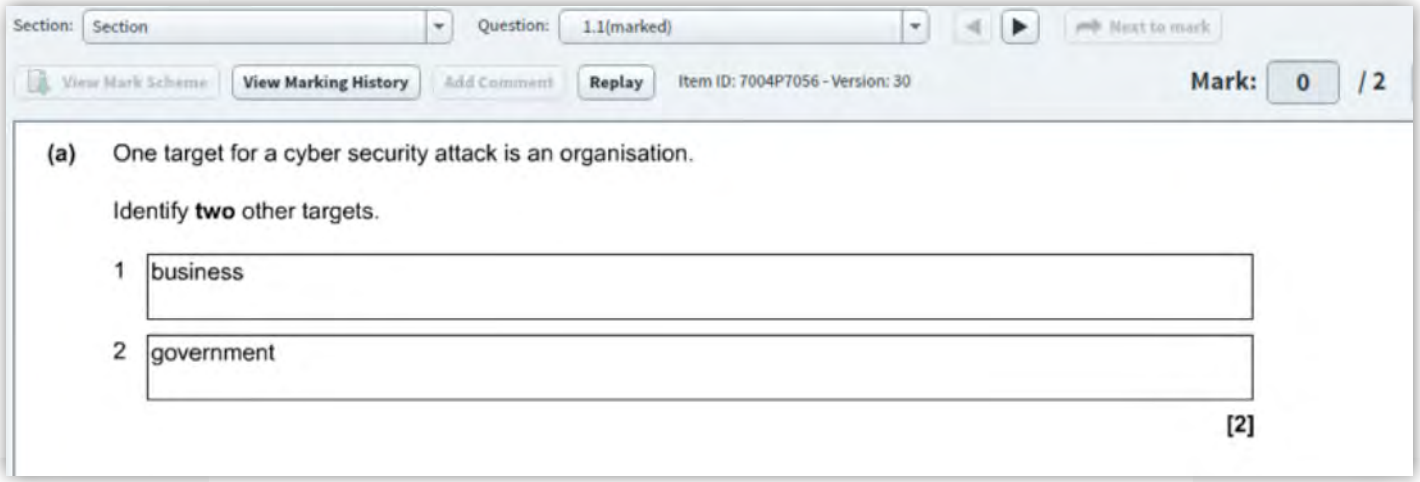
Question 1(a) – The focus of this question was on the different targets for cyber security attacks and ties into the list given in section 1.3 of the specification. Candidates frequently gave organisation, which was eliminated by the question.

Question 1(b) – This was generally done very well with the majority of candidates identifying phisher as the type of attacker.

Question 1(c) – This question focused on part 1.4 of the specification. Of the four types of cyber security incidents, two involve data loss. The majority of candidates were able to identify at least one of the incident types.

Exemplar candidate work

Question 1(a) – Low level answer



Commentary

The question required the candidates to provide two targets of a cyber security attack and can be referenced to LO1.3. Two targets are required for a question mark allocation of 2, each target is worth one mark. The keyword is 'identify' and as such a single word or phrase is an acceptable format for the answer.

The candidate has provided two incorrect answers – business and government. Acceptable answers, taken from the unit specification, include individuals, data/information and equipment. To improve this answer the candidate should provide two correct answers taken from this list.

Organisation is given in the question and, as such, is not an acceptable answer. If, as in this question, an example is provided in the question, candidates should ensure that they do not include this in their answers as this will not be considered for a mark.

Exemplar candidate work

Question 1(b) – Low level answer

Commentary

This question required candidates to identify the type of cyber attacker from a given description. The keyword is 'identify' and as such a single word or phrase is an acceptable format for the answer. The question is worth one mark.

The candidate has incorrectly identified the attacker as being a scammer. The correct answer for this question is a phisher.

Candidates should be able to identify the different types of cyber attacker, as listed in the unit specification, from a given description or provide a description of the listed cyber attackers.

Exemplar candidate work

Question 1(c) – Low level answer


View Mark Scheme | View Marking History | Add Comment | Replay | Item ID: 7004P7058 - Version: 23 | Mark: 0 / 2

(c) Data can be lost during a cyber security incident.

Identify **two** types of cyber security incidents where data is lost.

1 DoS

2 identity theft

[2]

Commentary

The question required the candidates to provide two types of cyber security incidents where data is lost. and can be referenced to LO1.4. Two targets are required for a question mark allocation of 2, each target is worth one mark. The keyword is 'identify' and as such a single word or phrase is an acceptable format for the answer.

The candidate has provided two incorrect answers – DoS and identity theft. Acceptable answers, taken from the unit specification, include data theft and data destruction. The other examples provided in the specification do not result in data being lost.

To improve this answer the candidate should provide two correct answers.

Questions 2(a) and (b)

View Mark Scheme | View Marking History | Add Comment | Replay

Mark: 0 / 1

A village is holding a sports day to raise funds for a children's playground.

A database of entries is created to contain details of the sports day competitors, their contact details, dates of birth and the classes entered. The database is stored on a laptop which has no protection measures.

(a) Identify the Act which relates to the holding of personal details.

- Data Protection Act/DPA (1)

[1]

View Mark Scheme | View Marking History | Add Comment | Replay

Mark: 0 / 2

(b) Describe how using access rights could increase the security of the database.

[2]

- Restricts what you can see (1) once unauthorised access has occurred (1)
- The tasks/example people can carry out (1) will be linked to their login details (1)
- Any other valid suggestion

Mark Scheme Guidance

Question 2(a):

Correct answer only.

Question 2(b):

Points marking approach.

One from list.

Examiner comments

Question 2(a) – It was disappointing that candidates were not aware of the data protection act –many gave computer misuse or a combination of words from different acts.

Question 2(b) – The focus of the question was on access rights and how they improve security. Many of the responses from candidates ignored this aspect and gave details about how security could be improved with the application of passwords, achieving no marks. It is important that time is spent by the candidate reading the question.

Questions 2(c), (d) and (e)

View Mark Scheme | View Marking History | Add Comment | Replay

Mark: 0 / 6

(c) Identify and describe **two** physical protection measures which could be used to protect the laptop.

1

2

- Biometric access device (1st) uses a fingerprint/example (1) to gain access to the laptop/ data held on it (1)
- Device lock (1st) (USB) ports are disabled (1) so no storage media can be used (1)
- Locked room/location (1st) the laptop is locked in room (1) with keys only available to authorised people (1)
- Any other valid suggestion

[6]

View Mark Scheme | View Marking History | Add Comment | Replay

Mark: 0 / 3

(d) Identify and describe **one** type of threat to individuals if the entry database is not kept secure.

- Identity theft (1st) personal details are stolen (1) and used for financial gain by another person/ example (1)
- Any other valid suggestion

[3]

View Mark Scheme | View Marking History | Add Comment | Replay

Mark: 0 / 4

(e) Describe **two** reasons why it is important to protect the personal data held in the entry database.

1

2

- If the data is lost/stolen then legal action could be taken against the organisers (1) as the data has not been kept secure (1)
- The people whose data has been stolen (1) may have to change bank details/notify authorities (1)
- People whose data has been stolen (1) can sue for compensation (1)
- Any other valid suggestion

[4]

Mark Scheme Guidance

Question 2(c):

The type of measure must be correct to enable marks for the description to be awarded.

1st mark for measure, up to 2 for description.

NOT security guards or CCTV.

Question 2(d):

The type of threat must be correct to enable marks for the description to be awarded.

Allow example of impact of threat OR example of data used in identity theft.

1st mark for threat, up to 2 for description.

Question 2(e):

Points marking approach.

Two from list.

Allow negative/reversed answers – "so that it is not used for …".

Examiner comments

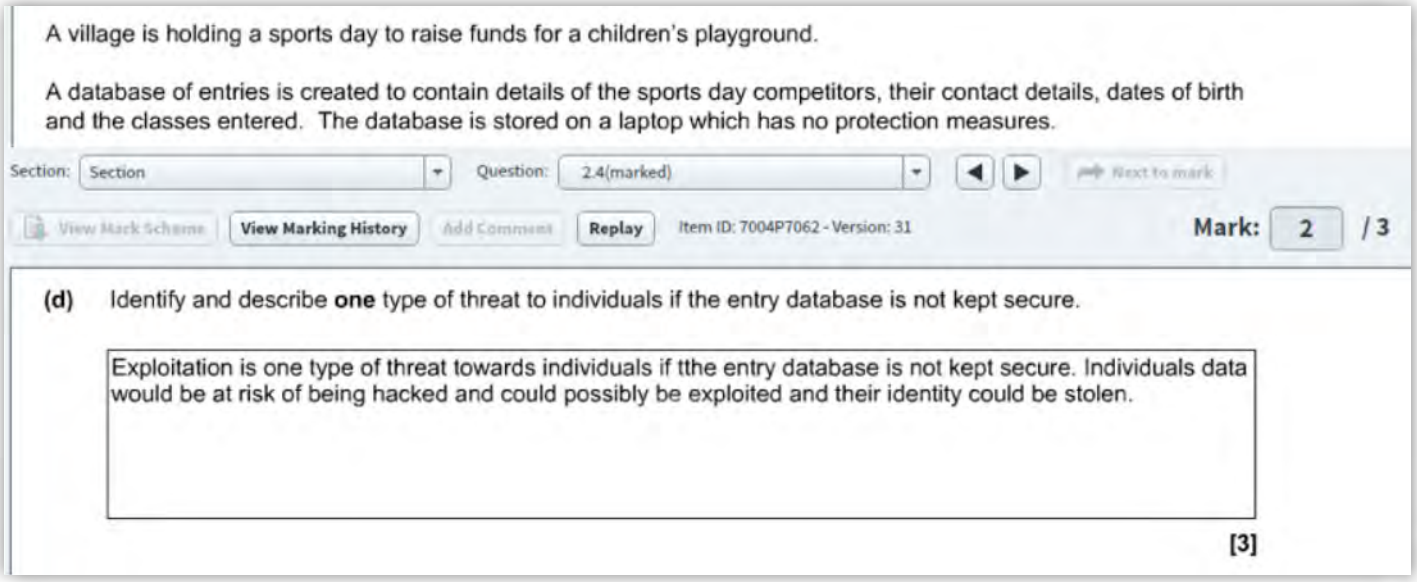
Question 2(c) – The difference between a physical and a logical security measure was not appreciated by the majority of candidates with answers given that were not related to physical security.

Question 2(d) – The types of threats are given in section 2.1 of the specification. Few candidates could give the one related to individuals. Without correct identification of the threat, the descriptive marks could not be obtained.

Question 2(e) – This question is at the core of cyber security, why we need to protect personal data and it was disappointing that the majority of candidates did not have an appreciation or understanding of this core aspect of the specification.

Exemplar candidate work

Question 2(d) – Medium level answer



A village is holding a sports day to raise funds for a children's playground.

A database of entries is created to contain details of the sports day competitors, their contact details, dates of birth and the classes entered. The database is stored on a laptop which has no protection measures.

Section: Section Question: 2.4(marked) Next to mark

View Mark Scheme | View Marking History | Add Comment | Replay | Item ID: 7004P7062 - Version: 31 | Mark: 2 / 3

(d) Identify and describe **one** type of threat to individuals if the entry database is not kept secure.

Exploitation is one type of threat towards individuals if tthe entry database is not kept secure. Individuals data would be at risk of being hacked and could possibly be exploited and their identity could be stolen.

[3]

Commentary

The question requires candidates to identify and describe one type of threat to individuals if the entry database is not kept secure. The question can be referenced to LO2.1.

The keywords for the question are 'identify and describe'. This means that candidates need to correctly identify a threat before they can be considered for marks for the description. One mark is allocated for the identification with the remaining two marks allocated for the description.

The candidate has identified that the identity could be stolen, so being awarded the identification mark. This means that the marks allocated for the description can be considered. The candidate has made some attempt at a description by saying that exploitation could take place. This can be awarded one mark out of the two allocated for the description.

To improve the answer, further description relating to the exploitation should be provided, such as an example of the type of exploitation that could happen.

Questions 3(a) and (b)

View Mark Scheme | View Marking History | Add Comment | **Replay** | **Mark: 0 / 2**

A school has a number of tablet computers.

The tablets will be used by students to carry out research using the internet and to access the school virtual learning platform. This platform is stored on a cloud storage area. The school also stores students' personal details, their progress and grades achieved in school and external assessments in a separate area in the same cloud storage area.

The cloud storage area has limited security measures. A user name and password are required for access. These provide access to all areas of the cloud storage area.

(a) Describe **one** reason why the school should increase the cyber security of the cloud storage area.

- Personal details are held (1) and these must be kept secure (1)
- If the cloud is hacked then students details/grades (1) could be taken/used by other people (1)
- Identity theft may occur (1) if personal details are hacked (1)
- Any other valid suggestion

[2]

Section: Section | Question: 3.2(not attempted) | Next to mark

View Mark Scheme | View Marking History | Add Comment | **Replay** | Item ID: 7004P7044 - Version: 21 | **Mark: 0 / 1**

(b) The webpage contains the owners' names and contact details and their pet's names.

(i) Identify the Act which covers the holding of these personal details.

- When users input the user name and password (1) a (one-time) token/number/code is sent/ emailed to the email account (1)
- Any other valid suggestion

[1]

Section: Section | Question: 3.3(not attempted) | Next to mark

View Mark Scheme | View Marking History | Add Comment | **Replay** | Item ID: 7004P7038 - Version: 21 | **Mark: 0 / 3**

(ii) Explain how having no security on this webpage breaks the Act you have identified in **part (i)**.

- Access rights (1st) the data/information that can be seen by people (1) is based on the log-in credentials (1)
- Firewalls (1st) unauthorised access (1) can be blocked (1)
- Encryption (1st) Data/information is unreadable (1) unless the user has the encryption key (1)
- Any other valid suggestion

[3]

Mark Scheme Guidance

Question 3(a):

Points marking approach.

Answers must relate to the security of the cloud and the information which is stored on it.

Question 3(b)(i):

Points marking approach.

Question 3(b)(ii):

The type of measure must be correct to enable marks for the description to be awarded.

1st mark for measure, up to 2 for description.

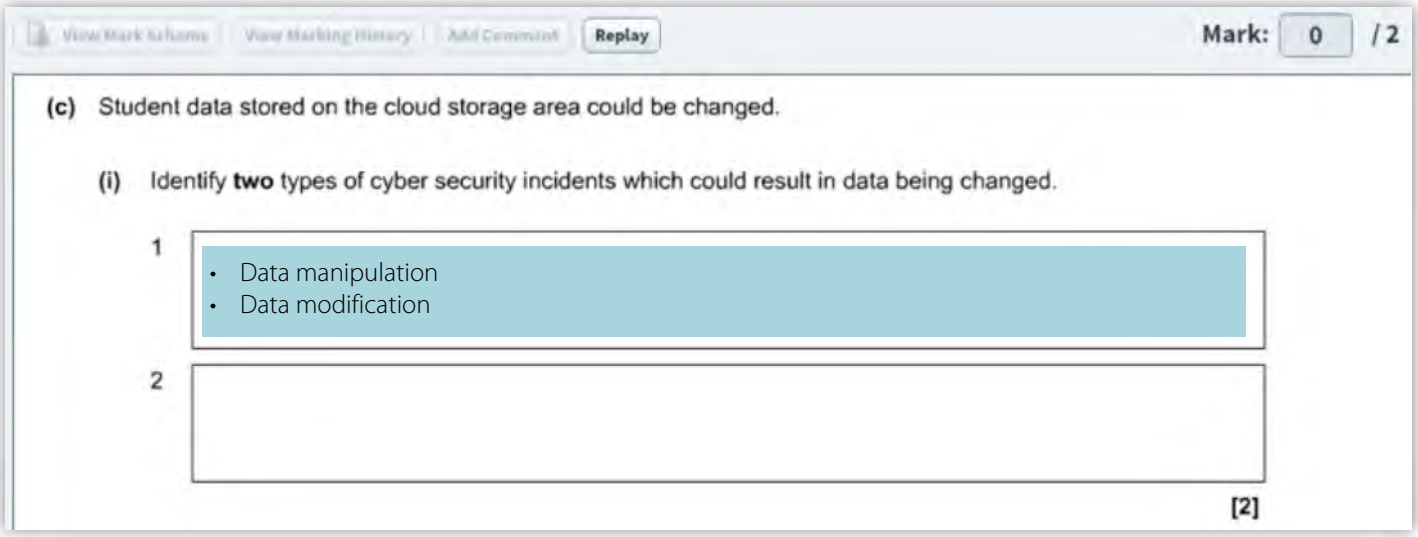
Examiner comments

Question 3(a) – The stem of the question gives some background to this question and its associated parts. One key piece of information is that the school has usernames and passwords currently in place. The focus of the question is on why they should increase the security. Many candidates gave responses based on security that could be applied, which in lots of cases included the use of passwords.

Question 3(b)(i) – The questions was asking for additional authentication that could be implemented, in addition to usernames and passwords. This was another question, which was not read by the candidates, and procedures based around passwords were given, including details on increasing complexity of passwords, which gained no marks.

Question 3(b)(ii) – The identification aspect of this question was answered reasonably well by many candidates, however few went on to give adequate descriptions.

Question 3(c)



View Mark Scheme | View Marking History | Add Comment | Replay | Mark: 0 / 2

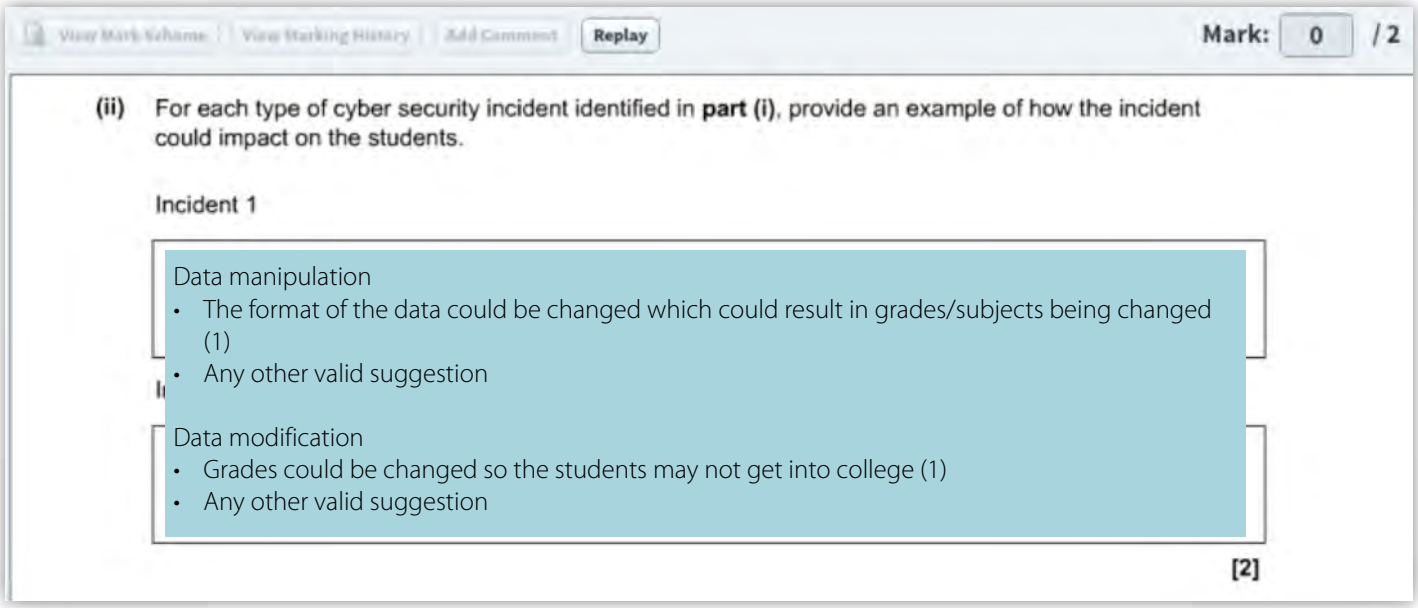
(c) Student data stored on the cloud storage area could be changed.

(i) Identify **two** types of cyber security incidents which could result in data being changed.

1
- Data manipulation
- Data modification

2

[2]



View Mark Scheme | View Marking History | Add Comment | Replay | Mark: 0 / 2

(ii) For each type of cyber security incident identified in **part (i)**, provide an example of how the incident could impact on the students.

Incident 1

Data manipulation
- The format of the data could be changed which could result in grades/subjects being changed (1)
- Any other valid suggestion

Data modification
- Grades could be changed so the students may not get into college (1)
- Any other valid suggestion

[2]

Mark Scheme Guidance

Question 3(c)(i):

Points marking approach

Two from list.

Question 3(c)(ii):

Points marking approach.

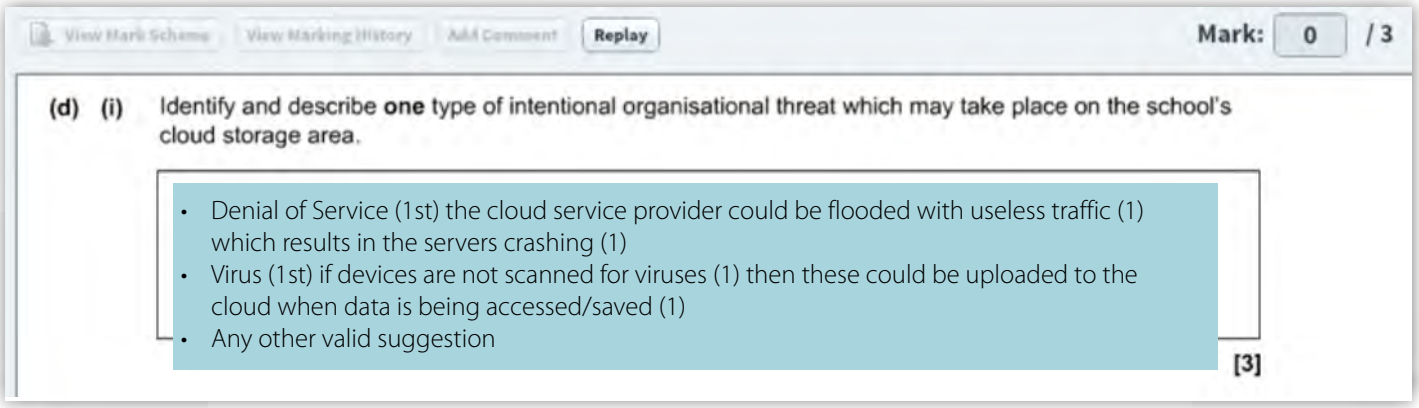
The answer must be focussed on the impact to the students.

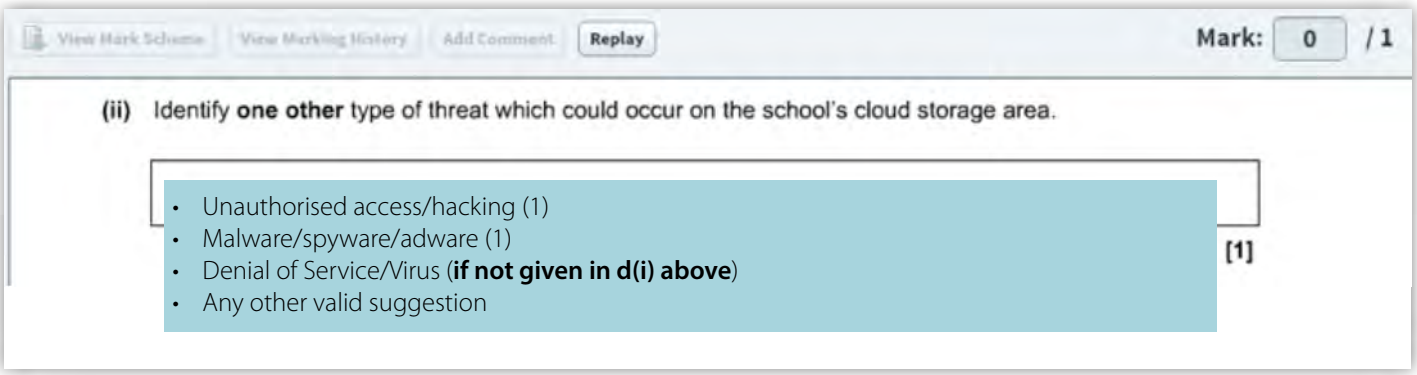
Examiner comments

Question 3(c)(i) – This question focused on part 1.4 of the specification. Of the four types of cyber security incidents, two involve data modification. Unfortunately, few candidates were able to identify these incident types.

Question 3(c)(ii) – This question is ties into the correct identification of the incident type. Without correct answers being obtained in Q3ci, marks cannot be obtained for this question. If the incidents were correctly identified, the candidates were being asked to apply their knowledge to the scenario given in the question. Whilst many used terms associated with schools, few were able to give specific examples that met the marking criteria.

Question 3(d)





Mark Scheme Guidance

Question 3(d)(i):

The type of threat must be correct to enable marks for the description to be awarded.

1st mark for threat, up to 2 for description.

Question 3(d)(ii):

Points marking approach.

One from list.

Examiner comments

Question 3(d)(i) – The focus of this question was twofold – organisational and intentional. Most candidates correctly identified hacking as one of the acceptable types, but often the expansion was lacking detail.

Question 3(d)(ii) – This question required the candidates to give an additional threat. Unfortunately, the majority of candidates only knew one threat and had given this in Q3di.

Question 3(e)

View Mark Scheme | View Marking History | Add Comment | Replay | Mark: 0 / 9

(e) Discuss the vulnerabilities which could lead to a cyber security attack on the cloud storage area.

[9]

Indicative content

Environmental
- Earthquakes could limit accessibility to cloud servers
- Updates in protection may not occur due to earthquakes/flooding and limiting of internet access
- Limited internet access may result in protection systems/encryption processes not being fully completed
- Any other valid suggestion.

Physical
- Theft of equipment which may have autofill password/usernames
- Unauthorised users accessing devices
- Any other valid suggestion.

System
- Hacking of devices
- Hacking of internet access device/router/hub
- Installation of malware/virus on device which can then self-replicate onto cloud
- Firewall/virus protection/anti-spyware out of date
- Any other valid suggestion.

Mark Scheme Guidance

Levels of response marking approach

7–9 marks

Learner has shown a detailed level of understanding by explaining the vulnerabilities which could occur. More than one vulnerability is explained in detail. Relevant and appropriate examples are provided.

Specialist terms will be used correctly and appropriately.

4–6 marks

Learner has shown a good level of understanding by describing the vulnerabilities which could occur. Descriptions may be limited in depth in the expansion(s).

Some relevant examples are provided although these may not always be appropriate.

Specialist terms will be used appropriately and for the most part correctly.

1–3 marks

Learner has identified points relevant to the vulnerabilities which could occur. This may take the form of a bulleted list.

Examples, if used, may lack relevance.

There will be little, if any, use of specialist terms.

0 marks

Nothing worthy of credit.

Examiner comments

Question 3(e) – This question was marked using a banded response method. Candidates were awarded marks based on the level of detail included in their response, and the application of their response to scenario. The question focused on the vulnerabilities that could lead to a cyber security attack – as this is part of question 3, it continues from the stem and hence the procedures that are currently in place. Therefore, responses relating to need for passwords gained no marks.

There are four main areas – environmental, physical, personnel and system with a variety of vulnerabilities that could have been discussed. The keyword discuss requires, for the top mark band, the candidates to show a detailed level of understanding by explaining the vulnerabilities which could occur. They would need to explain more than one vulnerability. There is also an expectation that relevant and appropriate examples are used by the candidate. Those candidates who did give suitable vulnerabilities often failed to give suitably detailed explanations. Many candidates took the "scattergun" approach, listing as many vulnerabilities as they know without giving the depth and detail required for each to move through the bands.

Exemplar candidate work

Question 3(e) – High level answer

View Mark Scheme | View Marking History | Add Comment | Replay | Item ID: 7004P7071 - Version: 24 | Mark: 7 / 9

(e) Discuss the vulnerabilities which could lead to a cyber security attack on the cloud storage area.

One vulnerbilites is that it can have is a physical effect. which mean that people can dowload an anti virus and steal the informaiton and can they can use the information in a bad way. to prevent this what the organisatoin can do is that they can install antivirus software which can stop the attack or they would allow denial of service to happen. For example hacker can install virus to cloud storage area and they can steal the data and the information that is in the storage.
Another vulnerbilities is that is have a securiy effect. This mean that people can hack into the cloud storage area if the user have an easy password. to prevent this they can do is that their password is a mixture of upper case and lower case,number and symbols. An example of this is that with cloud storage you would need a password so what most people is that they chose easy password such as therir names date of birth ot password1.This is the easier password that most people chose and it shows that hacker target individual that have have easy password. Hacker woudl cchose organisation that chose an easy password which make them a target.
another vulnerbilities is enviromental. This mean natual diaster can lead to a cyber security attatck.

[9]

Commentary

The question was marked using a levels of response method. The level awarded related to the level of detail included, the application of the response to a cloud storage area, the context for this question, and the correct, and appropriate, use of specialist terms.

The candidate has provided an answer which very clearly deals with three different types of vulnerabilities – physical, security and environmental. The discussion of the physical and security vulnerabilities are reasonably detailed however the discussion of the environmental vulnerability is limited in scope.

As the candidate has provided some discussion of three different types of vulnerabilities and provided some examples a mark in the highest level can be considered. However, as the discussion is limited in scope in some parts with limited use of specialist terms a mark at the bottom of the level is appropriate.

To move the answer further up the marks allocated for the highest level, a clear discussion of the three types of vulnerabilities including relevant examples should be present. In addition, specialist terms should be used appropriately and correctly.

The small print

We'd like to know your view on the resources we produce. By clicking on the 'Like' or 'Dislike' button you can help us to ensure that our resources work for you. When the email template pops up please add additional comments if you wish and then just click 'Send'. Thank you.

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/

ocr.org.uk/it

OCR Customer Contact 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

LLOYD'S REGISTER · LRQA
ISO 9001
UKAS MANAGEMENT SYSTEMS
001