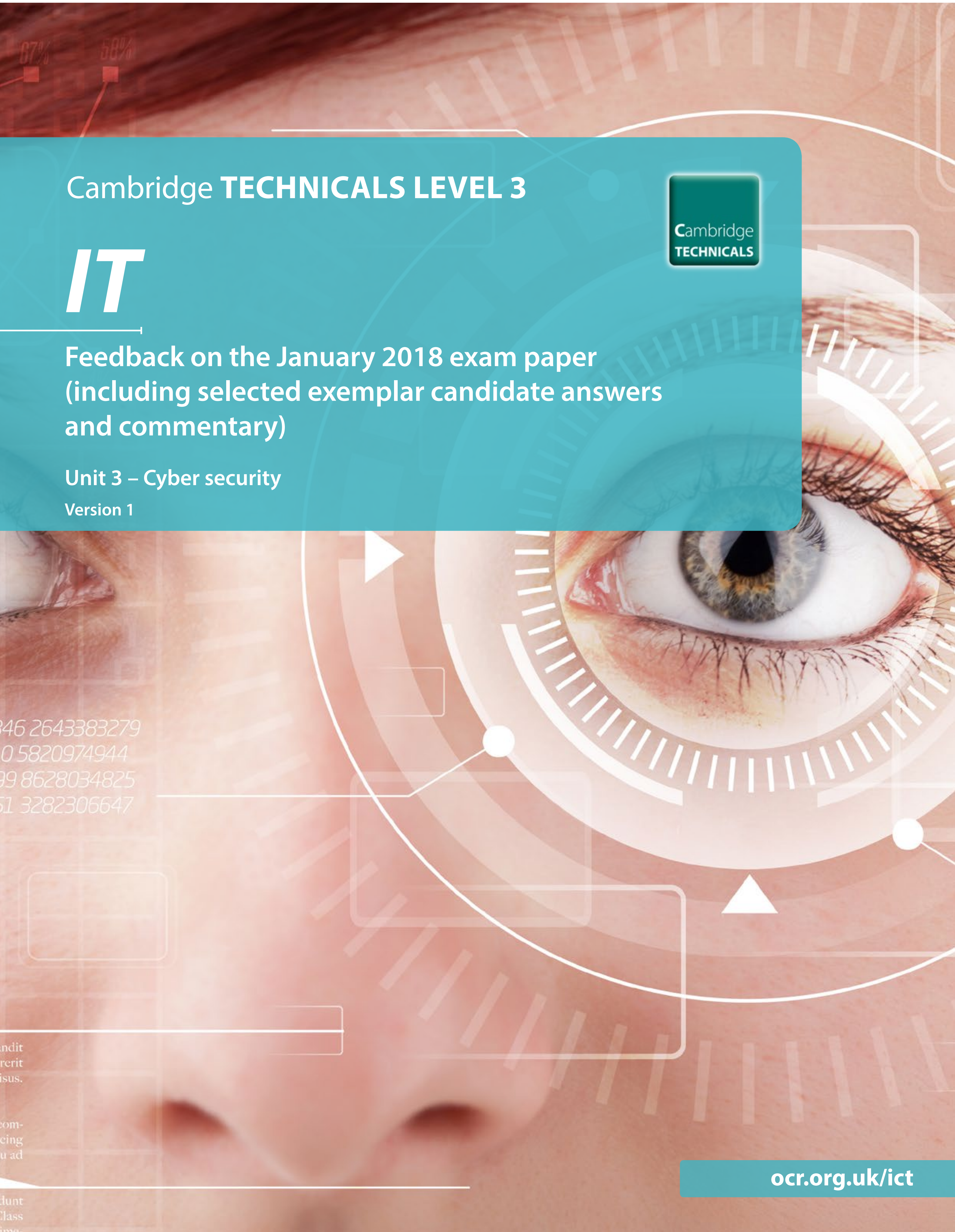
Cambridge **TECHNICALS LEVEL 3**

IT

Feedback on the January 2018 exam paper (including selected exemplar candidate answers and commentary)

Unit 3 – Cyber security

Version 1



ocr.org.uk/ict

CONTENTS

INTRODUCTION

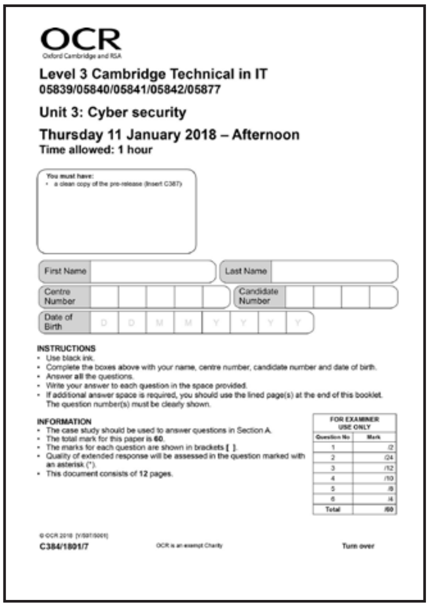
This resource brings together the questions from the January 2018 examined unit (Unit 3), the marking guidance, the examiners comments and the exemplar answers into one place for easy reference.

We have also included exemplar candidate answers with commentary for Questions 2(a), 2(d) and 6.

The marking guidance and the examiner's comments are taken from the Report to Centre for this question paper.

The Question Paper, Mark Scheme and the Report to Centre are available from:

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



OCR
Oxford Cambridge and RSA

Level 3 Cambridge Technical in IT
05839/05840/05841/05842/05877

Unit 3: Cyber security

Thursday 11 January 2018 – Afternoon
Time allowed: 1 hour

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

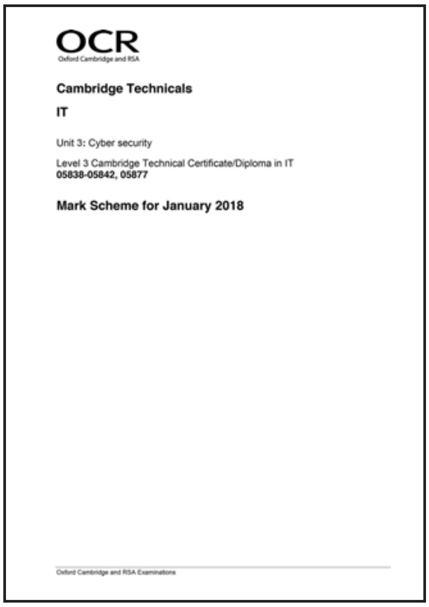
First Name		Last Name	
Centre Number		Candidate Number	
Date of Birth	D D M M Y Y Y Y		

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	/2
2	/24
3	/12
4	/10
5	/8
6	/4
Total	/60

© OCR 2018 [Y/507/5001]
C384/1801/7 OCR is an exempt Charity Turn over



OCR
Oxford Cambridge and RSA

Cambridge Technicals

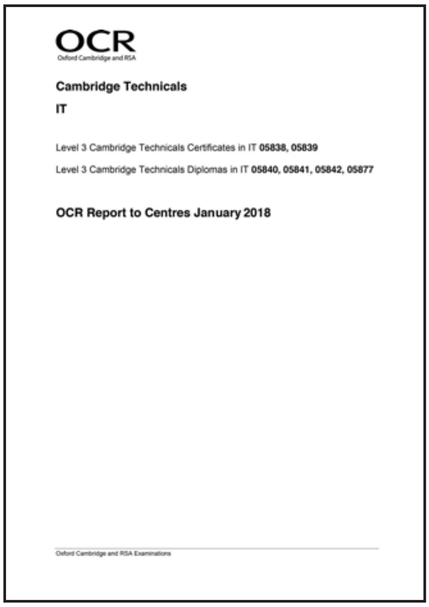
IT

Unit 3: Cyber security

Level 3 Cambridge Technical Certificate/Diploma in IT
05838-05842, 05877

Mark Scheme for January 2018

Oxford Cambridge and RSA Examinations



OCR
Oxford Cambridge and RSA

Cambridge Technicals

IT

Level 3 Cambridge Technicals Certificates in IT **05838, 05839**

Level 3 Cambridge Technicals Diplomas in IT **05840, 05841, 05842, 05877**

OCR Report to Centres January 2018

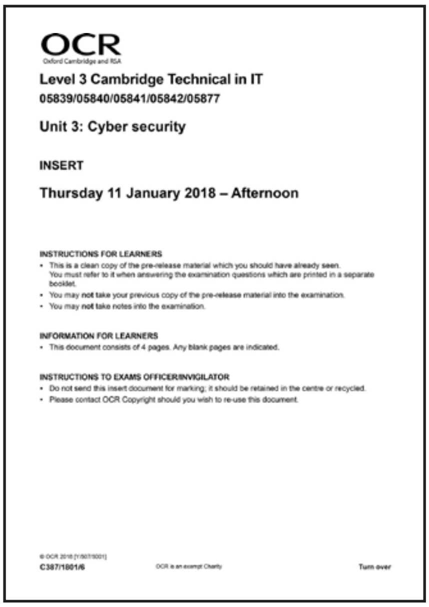
Oxford Cambridge and RSA Examinations

PRE-RELEASE MATERIAL

The question paper is based on a pre-release research brief which is issued to centres 6-8 weeks before the examination.

Learners should refer to this pre-release material to answer questions in the question paper.

The pre-release Research Brief can be found on Interchange.



OCR
Oxford Cambridge and RSA

Level 3 Cambridge Technical in IT
05839/05840/05841/05842/05877

Unit 3: Cyber security

INSERT

Thursday 11 January 2018 – Afternoon

INSTRUCTIONS FOR LEARNERS
- This is a clean copy of the pre-release material which you should have already seen. You must refer to it when answering the examination questions which are printed in a separate booklet.
- You may **not** take your previous copy of the pre-release material into the examination.
- You may **not** take notes into the examination.

INFORMATION FOR LEARNERS
- This document consists of 4 pages. Any blank pages are indicated.

INSTRUCTIONS TO EXAMS OFFICER/INVIGILATOR
- Do not send this insert document for marking; it should be retained in the centre or recycled.
- Please contact OCR Copyright should you wish to re-use this document.

© OCR 2018 [Y/507/5001]
C387/1801/6 OCR is an exempt Charity Turn over

GENERAL EXAMINER COMMENTS ON THE PAPER

Candidates seemed far better prepared both in terms of content and exam technique. The quality of answers were stronger and this was most marked in those answers requiring an extended answer. Candidates were also less likely to simply restate the question when answering or simply not attempting the question.

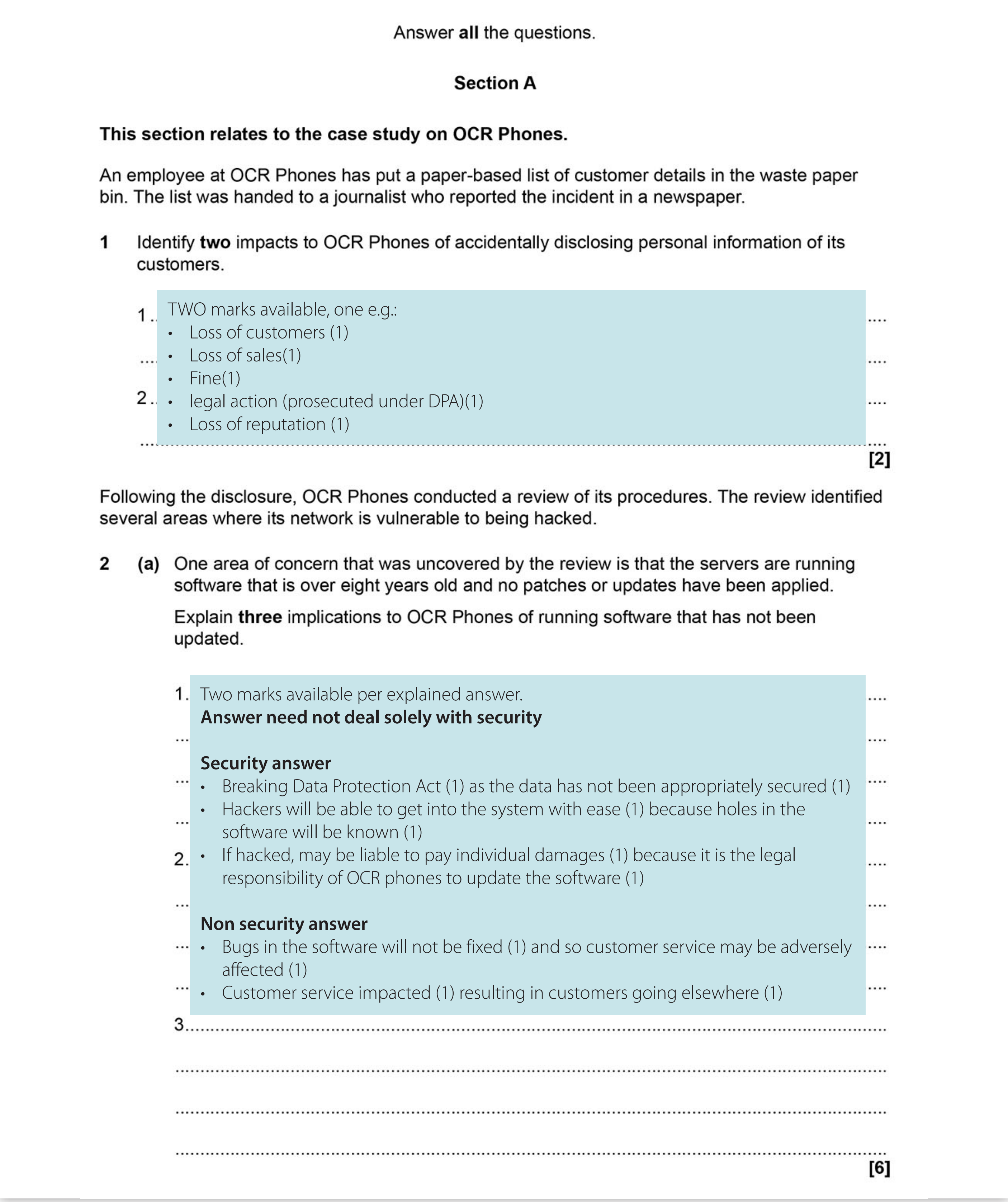
All of these factors contributed to a performance by the cohort that produced some excellent scripts with a good range of skills and understanding shown.

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 and 2(a)



Answer **all** the questions.

Section A

This section relates to the case study on OCR Phones.

An employee at OCR Phones has put a paper-based list of customer details in the waste paper bin. The list was handed to a journalist who reported the incident in a newspaper.

1 Identify **two** impacts to OCR Phones of accidentally disclosing personal information of its customers.

1 ....

2 ....

TWO marks available, one e.g.:

- Loss of customers (1)
- Loss of sales(1)
- Fine(1)
- legal action (prosecuted under DPA)(1)
- Loss of reputation (1)

[2]

Following the disclosure, OCR Phones conducted a review of its procedures. The review identified several areas where its network is vulnerable to being hacked.

2 **(a)** One area of concern that was uncovered by the review is that the servers are running software that is over eight years old and no patches or updates have been applied.

Explain **three** implications to OCR Phones of running software that has not been updated.

1 ....

2 ....

Two marks available per explained answer.
Answer need not deal solely with security

Security answer

- Breaking Data Protection Act (1) as the data has not been appropriately secured (1)
- Hackers will be able to get into the system with ease (1) because holes in the software will be known (1)
- If hacked, may be liable to pay individual damages (1) because it is the legal responsibility of OCR phones to update the software (1)

Non security answer

- Bugs in the software will not be fixed (1) and so customer service may be adversely affected (1)
- Customer service impacted (1) resulting in customers going elsewhere (1)

3 ....

....

....

....

[6]

Mark Scheme Guidance

Question 1:

Must be an impact on OCR phones and not to the customer.

"Customers lose faith/confidence" type answers can be accepted.

"Customers will be forced to shop elsewhere" type answers can NOT be accepted.

Accept any awareness of legal action.

Question 2(a):

Only award two marks for an answer where there is an explanation of the implications. Answers should usually be in the form of identify implication (1) explain the implication (1).

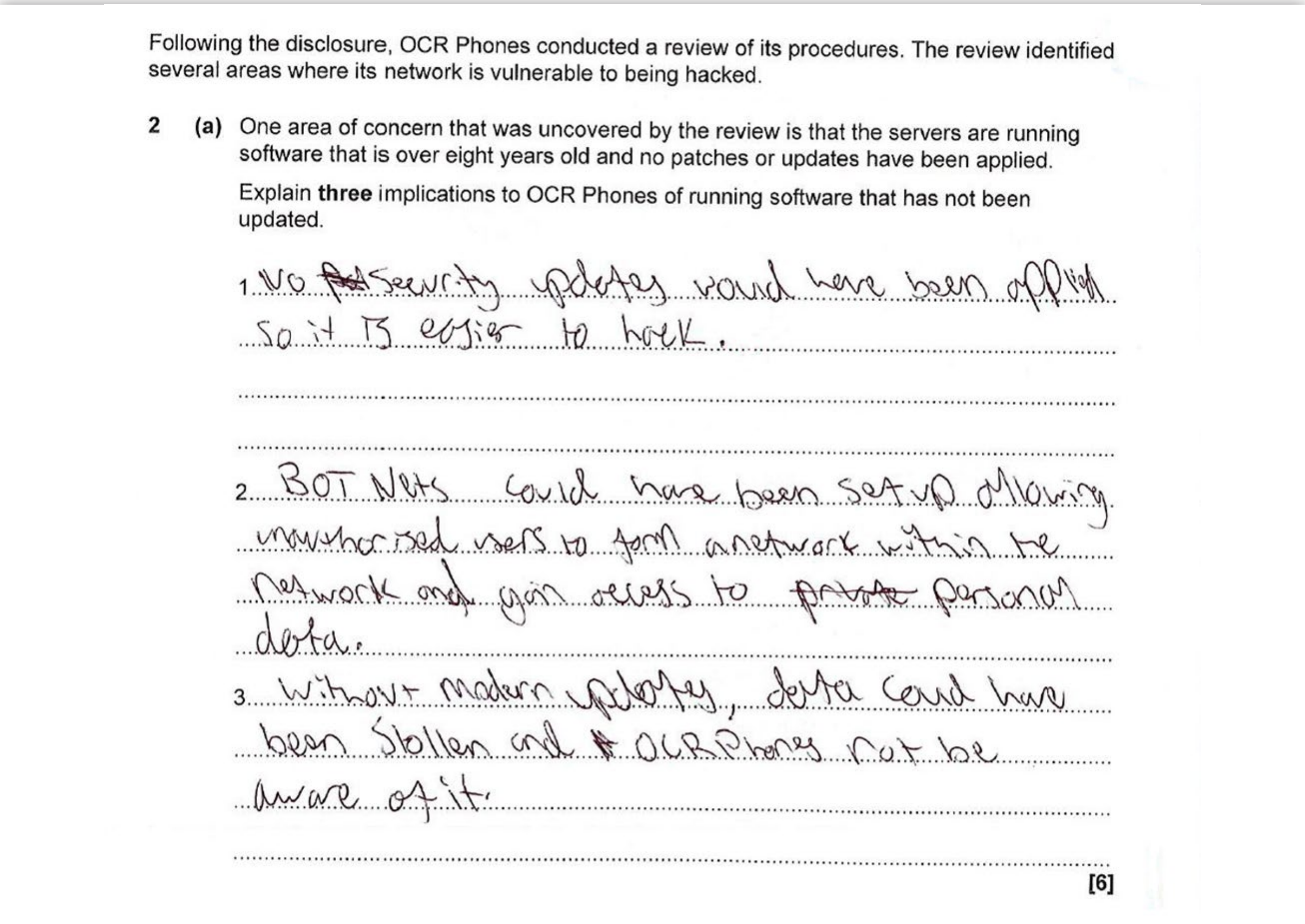
Examiner comments

Question 1 – This question was answered extremely well across the cohort as a whole, with the vast majority achieving full marks.

Question 2(a) – For question 2a, candidates did not need to focus solely on an e-safety implication of an out-of-date system and, indeed, candidates did identify the servers themselves would not be working as well as they should or were likely to be incompatible with other features of modern computing systems. Other answers obviously focussed on the cyber impact, but overall, question 2a was well answered.

Exemplar candidate work

Question 2(a) – Low level answer



Following the disclosure, OCR Phones conducted a review of its procedures. The review identified several areas where its network is vulnerable to being hacked.

2 (a) One area of concern that was uncovered by the review is that the servers are running software that is over eight years old and no patches or updates have been applied.

Explain **three** implications to OCR Phones of running software that has not been updated.

1 No Security updates would have been applied so it IS easier to hack.

2 BOT Nets could have been set up allowing unauthorised users to form a network within the network and gain access to ~~private~~ personal data.

3 Without modern updates, data could have been Stollen and OCR Phones not be aware of it.

[6]

Commentary

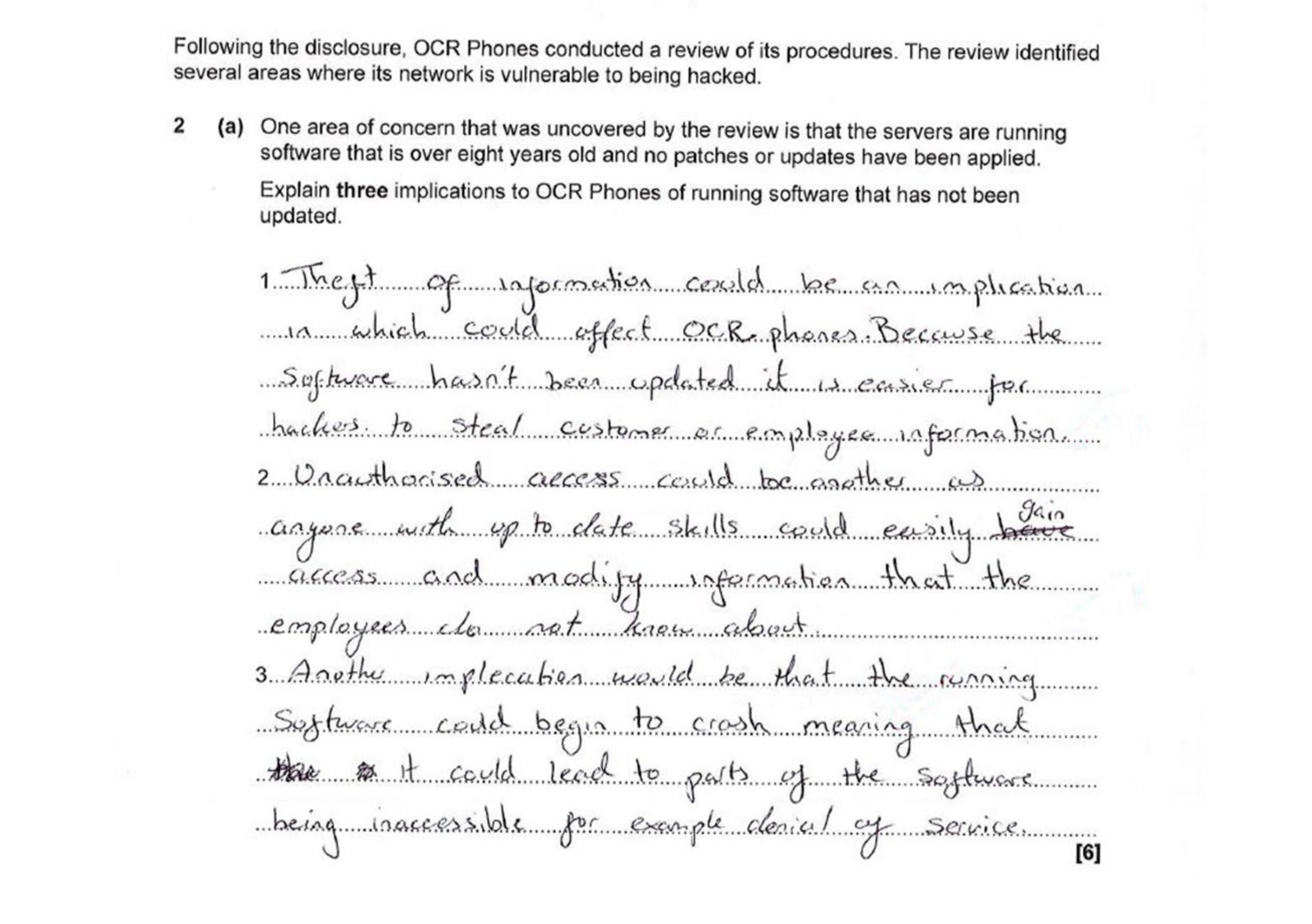
This is a low level answer because the candidate has identified one implication of the failure to update the software in the first section of the answer. Candidate has identified that the system would be easier to hack.

The question has asked to explain three implications. The suggested second and third implications are not acceptable as second section do not answer the question and third section is, at best, a weak repeat of the first point for which mark had already been awarded. Where the suggested implication was incorrect, no marks were available for the explanation.

In order to explain the implication, the candidate needed to have explained why it was an implication or how it had occurred, without repeating the question itself. For the first suggested explanation, the candidate has simply repeated the question as an attempt at an explanation and so has been awarded no marks for this section of the answer.

Exemplar candidate work

Question 2(a) – Medium level answer



Following the disclosure, OCR Phones conducted a review of its procedures. The review identified several areas where its network is vulnerable to being hacked.

2 (a) One area of concern that was uncovered by the review is that the servers are running software that is over eight years old and no patches or updates have been applied.

Explain **three** implications to OCR Phones of running software that has not been updated.

1. Theft of information could be an implication in which could affect OCR phones. Because the Software hasn't been updated it is easier for hackes. to steal customer or employee information.

2. Unauthorised access could be another as anyone with up to date skills could easily ~~have~~ gain access and modify information that the employees do not know about.

3. Anothe implecation would be that the running Software could begin to crash meaning that ~~the~~ ~~[illegible]~~ it could lead to parts of the Software being inaccessible for example denial of service.

[6]

Commentary

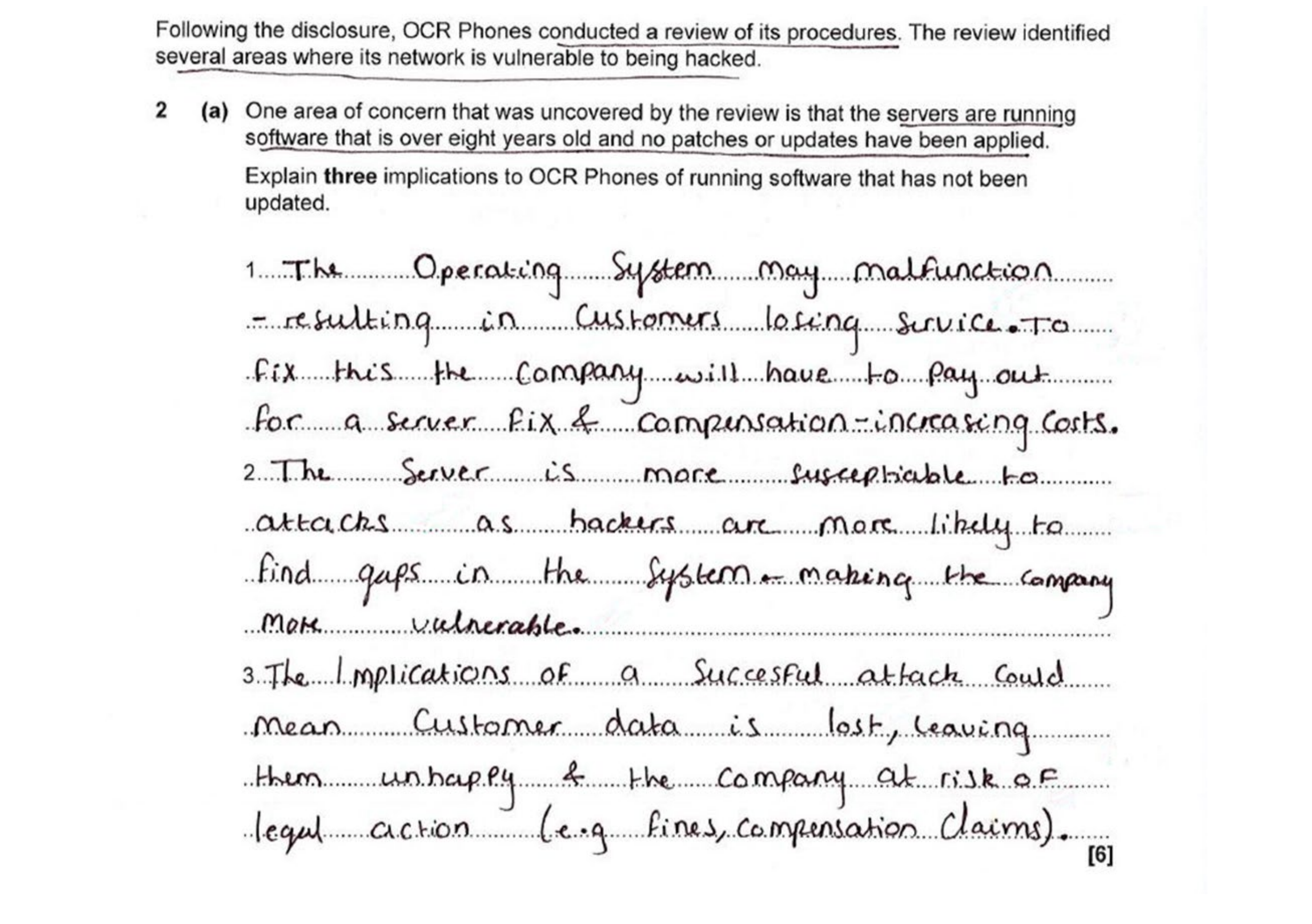
This candidate has identified three implications of the failure to update the software used. However, in the case of the first two answers, the candidate's explanation does not explain why it was an implication or how it had occurred. For example, why is it easier for hackers to steal customers' information if the software has not been updated? For answers 1 and 2, this is on the way to be being an explanation, but the candidate has not provided clear evidence that they know why their implication is an implication. The absence of this means that these answers cannot be awarded the explanation marks.

The third answer is a partial description of the implication (e.g. parts of the software would be inaccessible), but is not an explanation of why the software would crash or why it is an implication.

Had the candidate provided clear explanations, each of the three answers could have been awarded the full two marks.

Exemplar candidate work

Question 2(a) – High level answer



Following the disclosure, OCR Phones conducted a review of its procedures. The review identified several areas where its network is vulnerable to being hacked.

2 (a) One area of concern that was uncovered by the review is that the servers are running software that is over eight years old and no patches or updates have been applied.

Explain **three** implications to OCR Phones of running software that has not been updated.

1. The Operating System may malfunction - resulting in Customers losing service. To fix this the company will have to pay out for a server fix & compensation - increasing costs.

2. The Server is more susceptiable to attacks as hackers are more likely to find gaps in the System - making the company more vulnerable.

3. The Implications of a succesful attack could mean Customer data is lost, leaving them unhappy & the company at risk of legal action (e.g fines, compensation claims).

[6]

Commentary

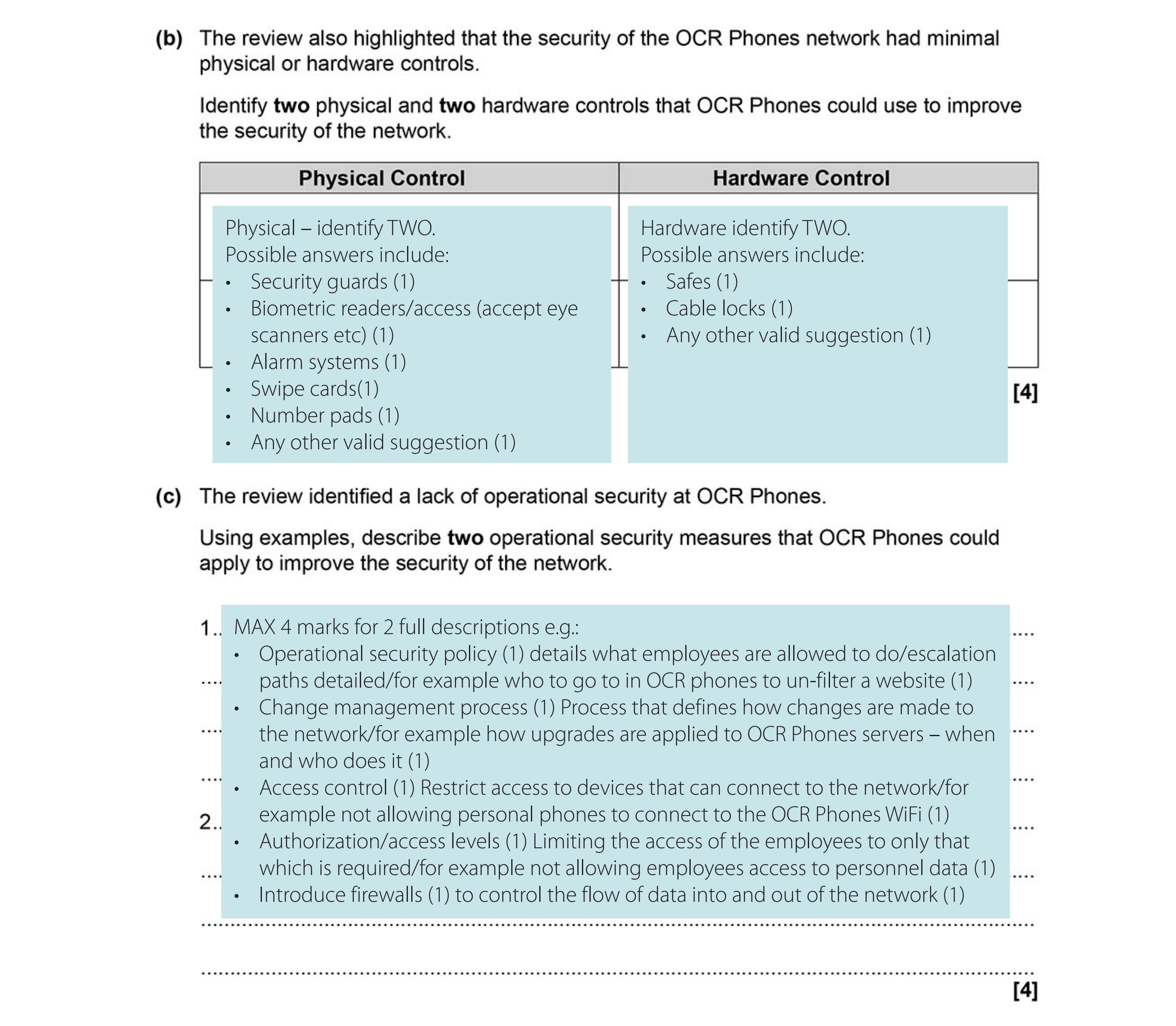
The difference in quality between this answer and the previous example is the extent to which the candidate has shown clear understanding of why the implication has been caused or why it is an implication.

In the first section, the candidate has stated that the software may malfunction and lose data, which would then have a cost implication. This is a well-structured answer that shows good understanding.

Similarly, second section gives a well-structured answer. It show that the candidate is aware of the lack of update does mean that hackers will have found gaps in security and so the company is more vulnerable. This answer could have been better developed by explaining that the lack of updates over time has given hackers more opportunity to find gaps in security, or that gaps may already have been identified on other systems, but overall, this explanation is worth 2 marks.

The third section shows a clear explanation of the loss of data and the consequent exposure to legal action.

Questions 2(b) and (c)



(b) The review also highlighted that the security of the OCR Phones network had minimal physical or hardware controls.

Identify **two** physical and **two** hardware controls that OCR Phones could use to improve the security of the network.

Physical Control	Hardware Control
Physical – identify TWO. Possible answers include: • Security guards (1) • Biometric readers/access (accept eye scanners etc) (1) • Alarm systems (1) • Swipe cards(1) • Number pads (1) • Any other valid suggestion (1)	Hardware identify TWO. Possible answers include: • Safes (1) • Cable locks (1) • Any other valid suggestion (1)

[4]

(c) The review identified a lack of operational security at OCR Phones.

Using examples, describe **two** operational security measures that OCR Phones could apply to improve the security of the network.

1.

2.

MAX 4 marks for 2 full descriptions e.g.:

- Operational security policy (1) details what employees are allowed to do/escalation paths detailed/for example who to go to in OCR phones to un-filter a website (1)
- Change management process (1) Process that defines how changes are made to the network/for example how upgrades are applied to OCR Phones servers – when and who does it (1)
- Access control (1) Restrict access to devices that can connect to the network/for example not allowing personal phones to connect to the OCR Phones WiFi (1)
- Authorization/access levels (1) Limiting the access of the employees to only that which is required/for example not allowing employees access to personnel data (1)
- Introduce firewalls (1) to control the flow of data into and out of the network (1)

[4]

Mark Scheme Guidance

Question 2(b):

Cameras do not improve security, they monitor.

Do not allow repetition of answers across control types.

Question 2(c):

Identify operational security measure (1) plus example of that measure as applied (1).

There is no need to identify OCR phone by name.

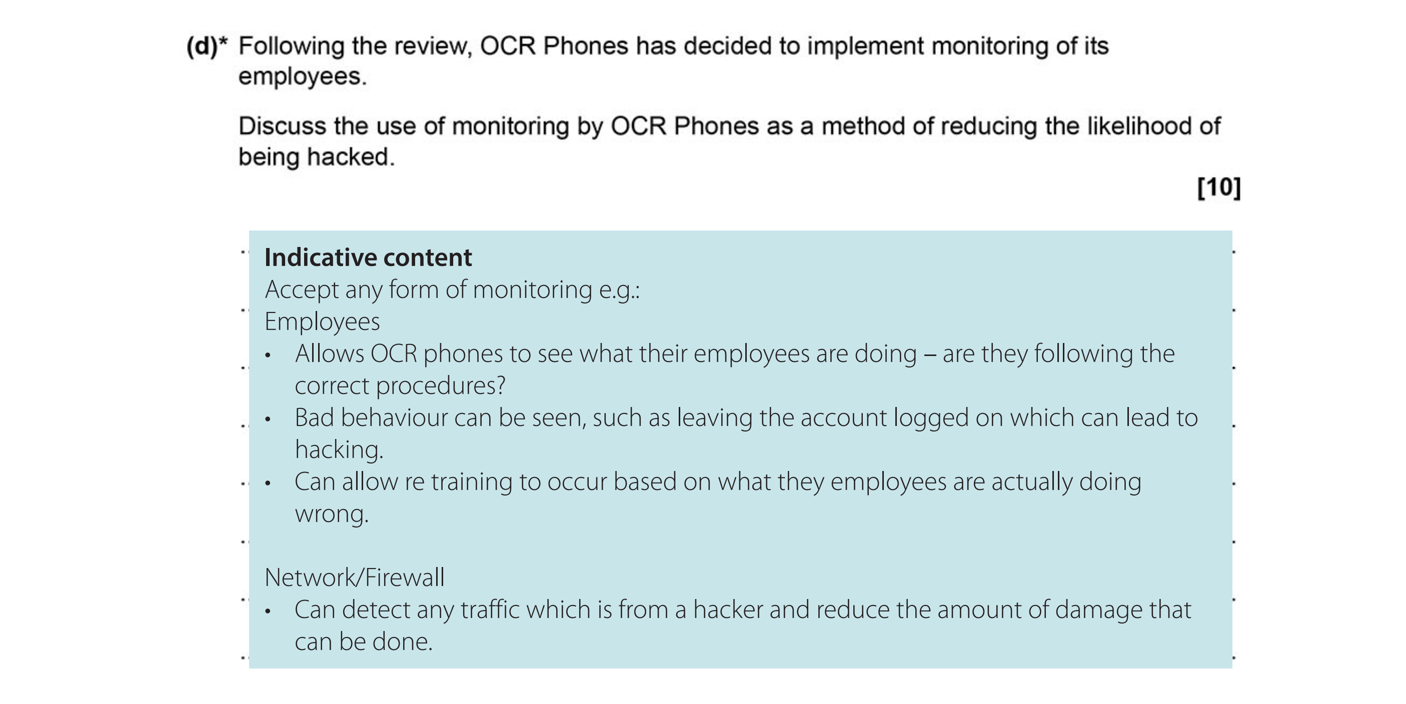
Accept any change to working procedure (day to day or longer term) (operational practice) to increase security of the network (by implication, this includes data on that network).

Examiner comments

Question 2(b) – brought some interesting answers, but the majority of candidates were able to identify at least one example of both physical and hardware controls.

Question 2(c) –For question 2c, candidates had to identify operational security measures. A good proportion of candidates correctly described operational security measures but others missed the focus of the question and gave general measures that were not considered to be operational.

Question 2(d)



(d)* Following the review, OCR Phones has decided to implement monitoring of its employees.

Discuss the use of monitoring by OCR Phones as a method of reducing the likelihood of being hacked.

[10]

Indicative content

Accept any form of monitoring e.g.:

Employees

- Allows OCR phones to see what their employees are doing – are they following the correct procedures?
- Bad behaviour can be seen, such as leaving the account logged on which can lead to hacking.
- Can allow re training to occur based on what they employees are actually doing wrong.

Network/Firewall

- Can detect any traffic which is from a hacker and reduce the amount of damage that can be done.

Mark Scheme Guidance

Level 3: 7–10 marks

Has shown a detailed level of understanding by discussing the use of monitoring as a method of reducing the likelihood of being hacked. The learner provides a clear discussion of more than one clear implication.

Relevant examples will be used to support discussion and ideas will be expressed clearly and fluently.

There is a well-developed line of reasoning which is clear and logically structured. The information presented is relevant and substantiated.

Level 2: 4–6 marks

Has shown a good level of understanding by explaining the use of monitoring by OCR Phones as a method of reducing the likelihood of being hacked. Explanations may concentrate on one implication, with, at the lower end of the mark band, limited depth.

Some examples used to support discussion may not be relevant and may at times detract from fluency of narrative.

There will be a line of reasoning presented with some structure. The information presented is in the most part relevant and supported by some evidence.

Level 1: 1–3 marks

Has identified points relevant to the use of monitoring to reduce the likelihood of being hacked. Limited use of examples to accompany description and ideas poorly expressed.

The information is basic and is communicated in an unstructured way. The information is supported by limited evidence and the relationship to the evidence may not be clear.

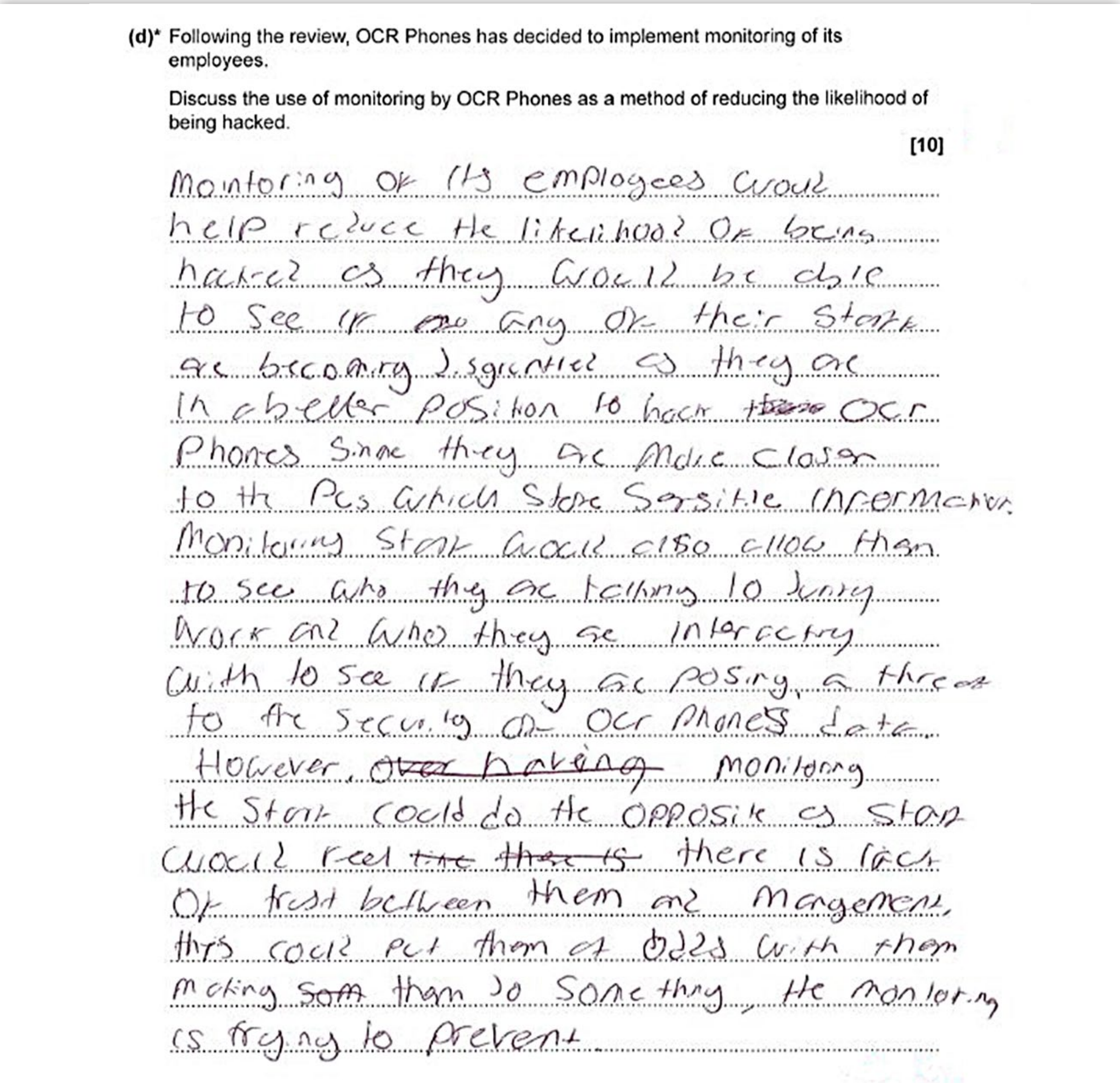
0 marks – Nothing worthy of credit.

Examiner comments

Question 2(d) – asked candidates to discuss the use of monitoring of employees as a method whereby the likelihood of hacking could be reduced. As mentioned above, the quality of writing displayed in answer to this question was far superior to that seen in previous series. However, even with a range of different methods of monitoring accepted by markers, some candidates managed to write answers that were either wrong in their interpretation or so lacking in focus on monitoring as to make marks difficult to allocate. That having been said, this question was generally well answered.

Exemplar candidate work

Question 2(d) – Medium level answer



(d)* Following the review, OCR Phones has decided to implement monitoring of its employees.

Discuss the use of monitoring by OCR Phones as a method of reducing the likelihood of being hacked.

[10]

Monitoring of its employees would help reduce the likelihood of being hacked as they would be able to see if ~~an~~ any of their staff are becoming disgruntled as they are in a better position to hack ~~the~~ OCR Phones since they are more closer to the PCs which store sensitive information. Monitoring staff would also allow them to see who they are talking to during work and who they are interacting with to see if they are posing a threat to the security of OCR Phones data.

However, ~~over hacking~~ monitoring the staff could do the opposite as staff would feel ~~the there is~~ there is lack of trust between them and management, this could put them at odds with them making ~~som~~ them do something the monitoring is trying to prevent.

Commentary

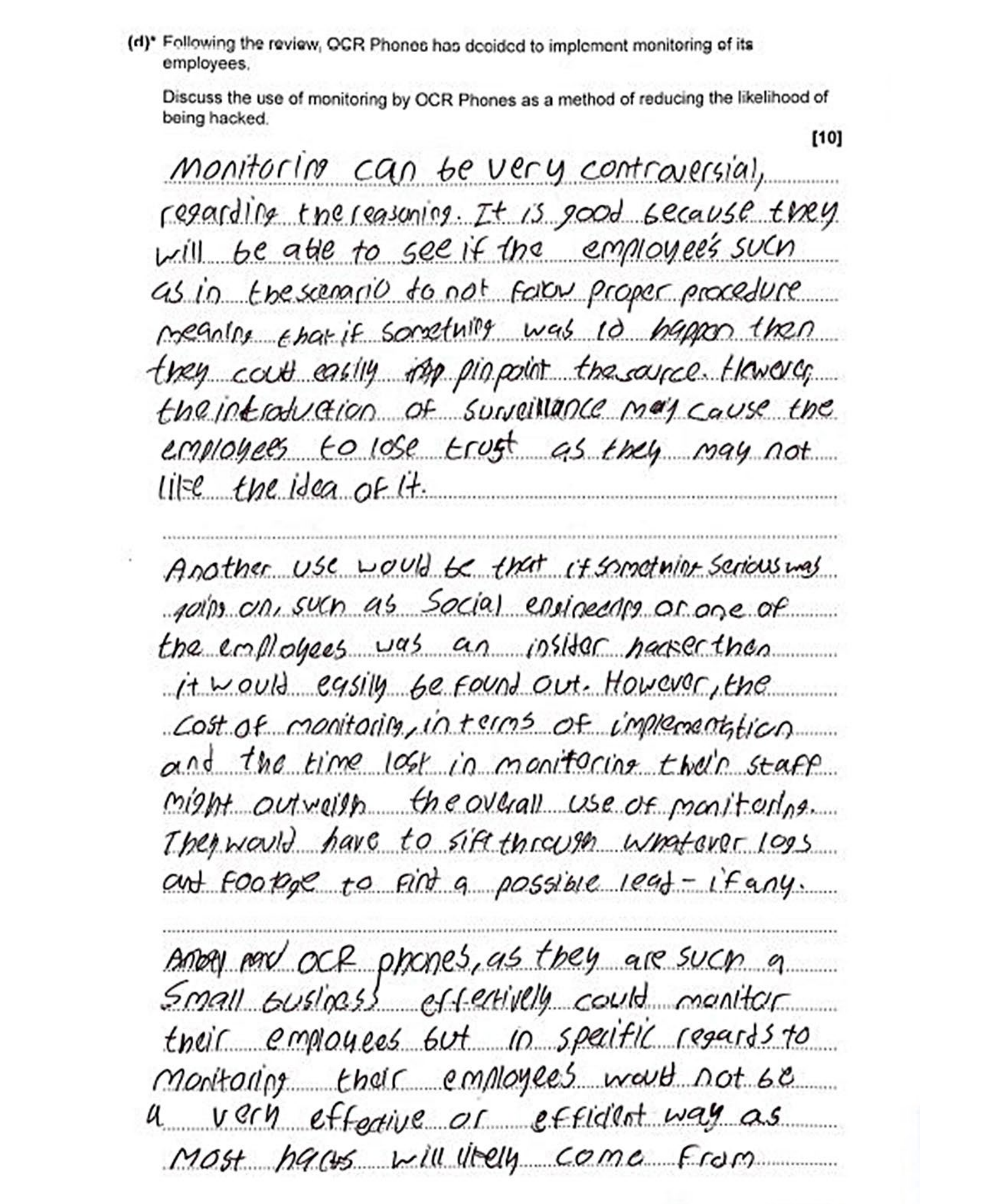
The first point to note here is that this question has been assessed on the use of language as well as on the subject knowledge.

The answer itself is presented almost as a flow of consciousness and is lacking in detail. Two relevant positive implications and one relevant negative have been identified, with some explanation. However, overall this is vague. The reference to "making them do something the monitoring is trying to prevent" in the final paragraph is a good example of this lack of clarity.

Had the candidate presented this with a slightly better structure, the full marks for MB2 would have been given. The use of examples, and a good deal with more clarity, would have been needed to make this answer a high level answer.

Exemplar candidate work

Question 2(d) – High level answer



(d)* Following the review, OCR Phones has decided to implement monitoring of its employees.

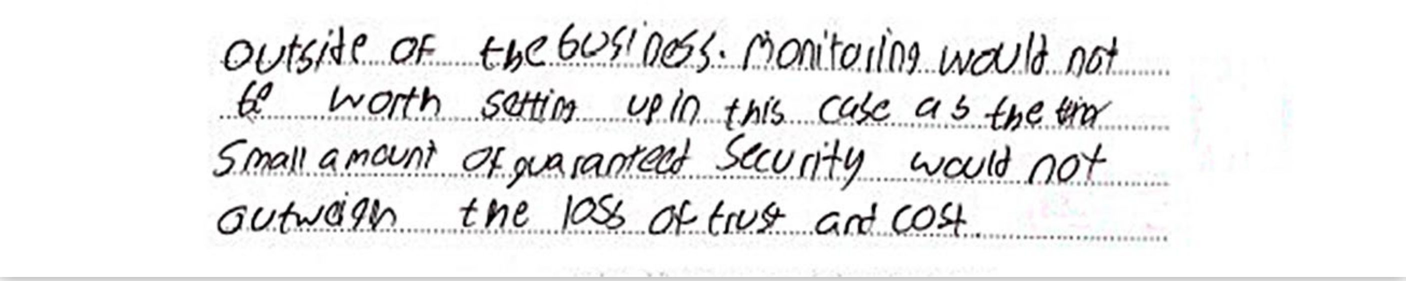
Discuss the use of monitoring by OCR Phones as a method of reducing the likelihood of being hacked.

[10]

Monitoring can be very controversial, regarding the reasoning. It is good because they will be able to see if the employee's such as in the scenario do not follow proper procedure meaning that if something was to happen then they could easily ~~[illegible]~~ pin point the source. However, the introduction of surveillance may cause the employees to lose trust as they may not like the idea of it.

Another use would be that if something serious was going on, such as social engineering or one of the employees was an insider hacker then it would easily be found out. However, the cost of monitoring, in terms of implementation and the time lost in monitoring their staff might outweigh the overall use of monitoring. They would have to sift through whatever logs and footage to find a possible lead - if any.

~~[illegible]~~ OCR phones, as they are such a small business effectively could monitor their employees but in speific regards to monitoring their employees would not be a very effective or efficient way as most hacks will likely come from



outside of the business. Monitoring would not
be worth setting up in this case as the ~~tiny~~
small amount of guaranted security would not
outweigh the loss of trust and cost

Commentary

The difference in standard between high level example and the previous example of a medium level answer is clear. This candidate's answer has a structure and a clarity that is missing in that of the previous candidate.

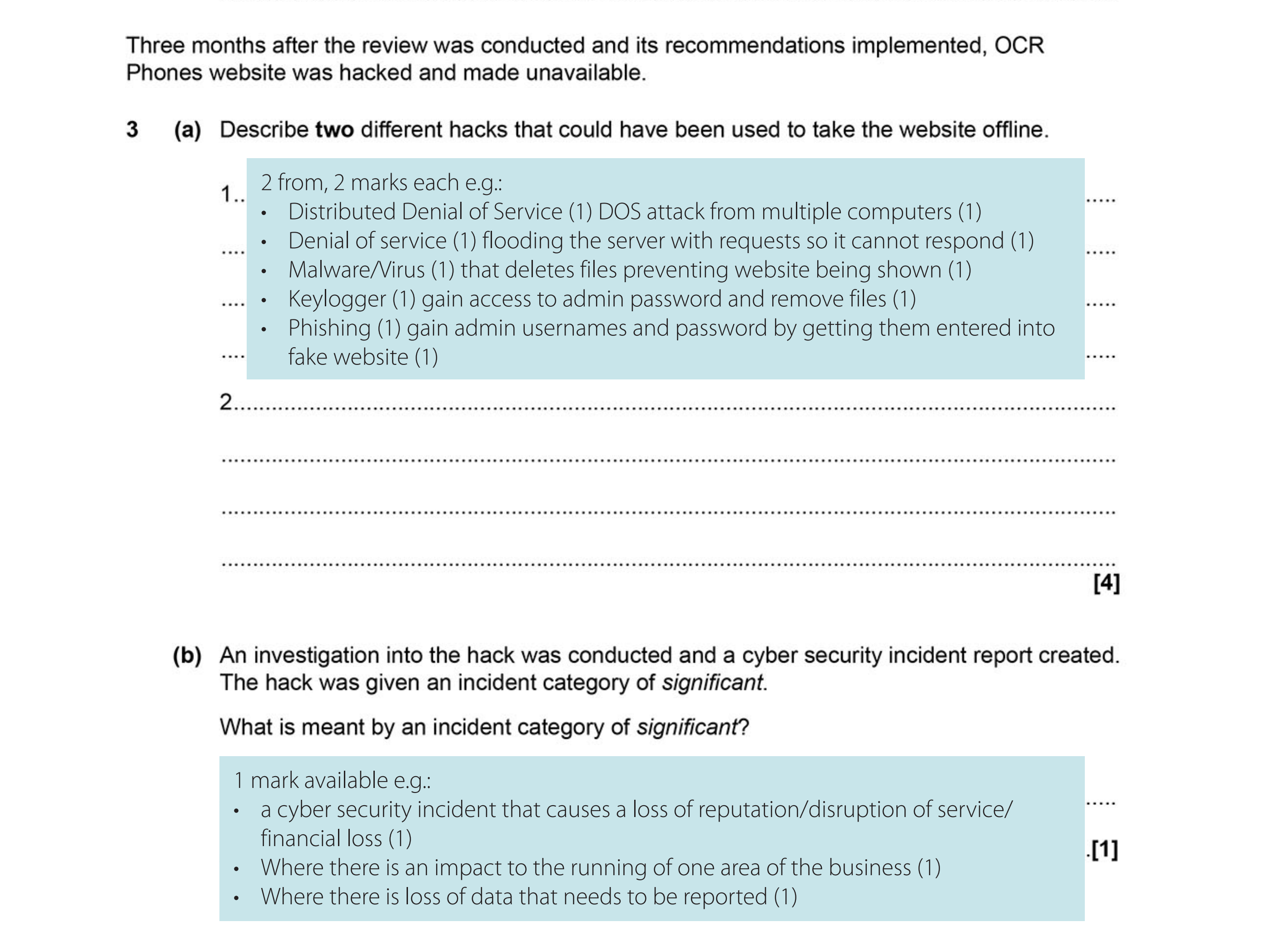
The discussion itself makes a series of points, all of which are relevant. The fact that the candidate has attempted (and succeeded) in making matched dialectical comments. The discussion shows a good level of understanding with detailed answer. In the first paragraph, the candidate has made a strong claim at the start and then proceeded to show why the use of monitoring is controversial. The second part of this paragraph is not as effective as the first, as the first is clear why the use of monitoring is positive, but the opposing argument is not as well made.

For paragraph two, the candidate makes two points. It reads like a good answer but lacks amount of depth required. Especially the second point about the cost-benefit analysis which would have been better placed in the conclusion that the candidate has given.

The final closing points are not as strongly made as those made at the start of the answer. There is an assumption that most hacks would come from outside of the business and therefore, the cost of any monitoring is largely a waste.

Overall, this answer has some really good points made, but loses its way slightly in the second paragraph and then ends with a poorly argued conclusion. The candidate clearly has an understanding of the issues; the answer itself is fairly well structured and there are examples, although these could be improved. This answer is a high level answer, but is lacking the full clarity, structure and use of examples required for a full mark answer.

Questions 3(a) and (b)



Three months after the review was conducted and its recommendations implemented, OCR Phones website was hacked and made unavailable.

3 **(a)** Describe **two** different hacks that could have been used to take the website offline.

1..

2 from, 2 marks each e.g.:
- Distributed Denial of Service (1) DOS attack from multiple computers (1)
- Denial of service (1) flooding the server with requests so it cannot respond (1)
- Malware/Virus (1) that deletes files preventing website being shown (1)
- Keylogger (1) gain access to admin password and remove files (1)
- Phishing (1) gain admin usernames and password by getting them entered into fake website (1)

2...

....

....

....

[4]

(b) An investigation into the hack was conducted and a cyber security incident report created. The hack was given an incident category of *significant*.

What is meant by an incident category of *significant*?

1 mark available e.g.:
- a cyber security incident that causes a loss of reputation/disruption of service/ financial loss (1)
- Where there is an impact to the running of one area of the business (1)
- Where there is loss of data that needs to be reported (1)

[1]

Mark Scheme Guidance

Question 3(b):

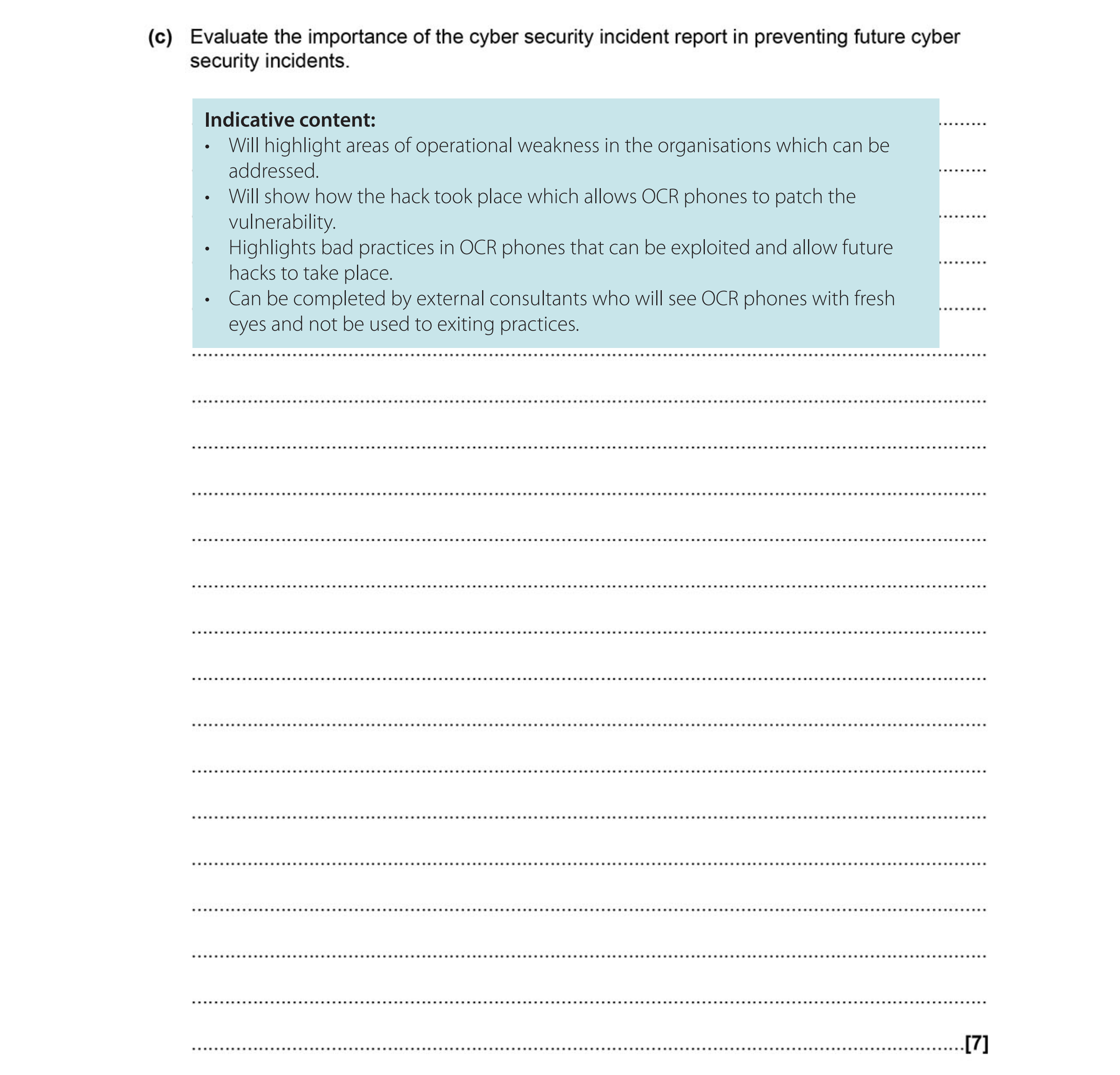
Accept examples where relevant.

Examiner comments

Question 3(a) – For question 3a, markers relaxed their interpretation of a 'hack' and instead focussed on whether the attack could take a website off line. The majority of candidates correctly identified and described a DNS attack, whilst the second most frequent answer was a DDNS attack. Where the description of the DDNS attack was not a repeat of the DNS description, but focussed on the distributed nature of the attack, full marks were awarded.

Question 3(b) –Across the cohort, this part of the question was well answered. However, question 3b proved more of a challenge. Some candidates stated that 'significant' was an indication of how important the attack was and so were really simply repeating the question, whilst others attempted to give examples. Where candidates talked about impact on data, or an impact on the ability of the business to function, marks were awarded.

Question 3(c)



(c) Evaluate the importance of the cyber security incident report in preventing future cyber security incidents.

Indicative content:

- Will highlight areas of operational weakness in the organisations which can be addressed.
- Will show how the hack took place which allows OCR phones to patch the vulnerability.
- Highlights bad practices in OCR phones that can be exploited and allow future hacks to take place.
- Can be completed by external consultants who will see OCR phones with fresh eyes and not be used to exiting practices.

[7]

Mark Scheme Guidance

Level of response marking approach

Level 3: 5–7 marks

Has shown a detailed level of understanding by explaining the importance of the report in preventing future incidents.

A conclusion may be given but may be implied. Relevant examples will be used to support explanation.

Level 2: 3–4 marks

Has shown a good level of understanding by describing the importance of the report in preventing future incidents.

Some examples used to support description but may not be relevant.

Level 1: 1–2 marks

Has identified points relevant to the importance of the report.

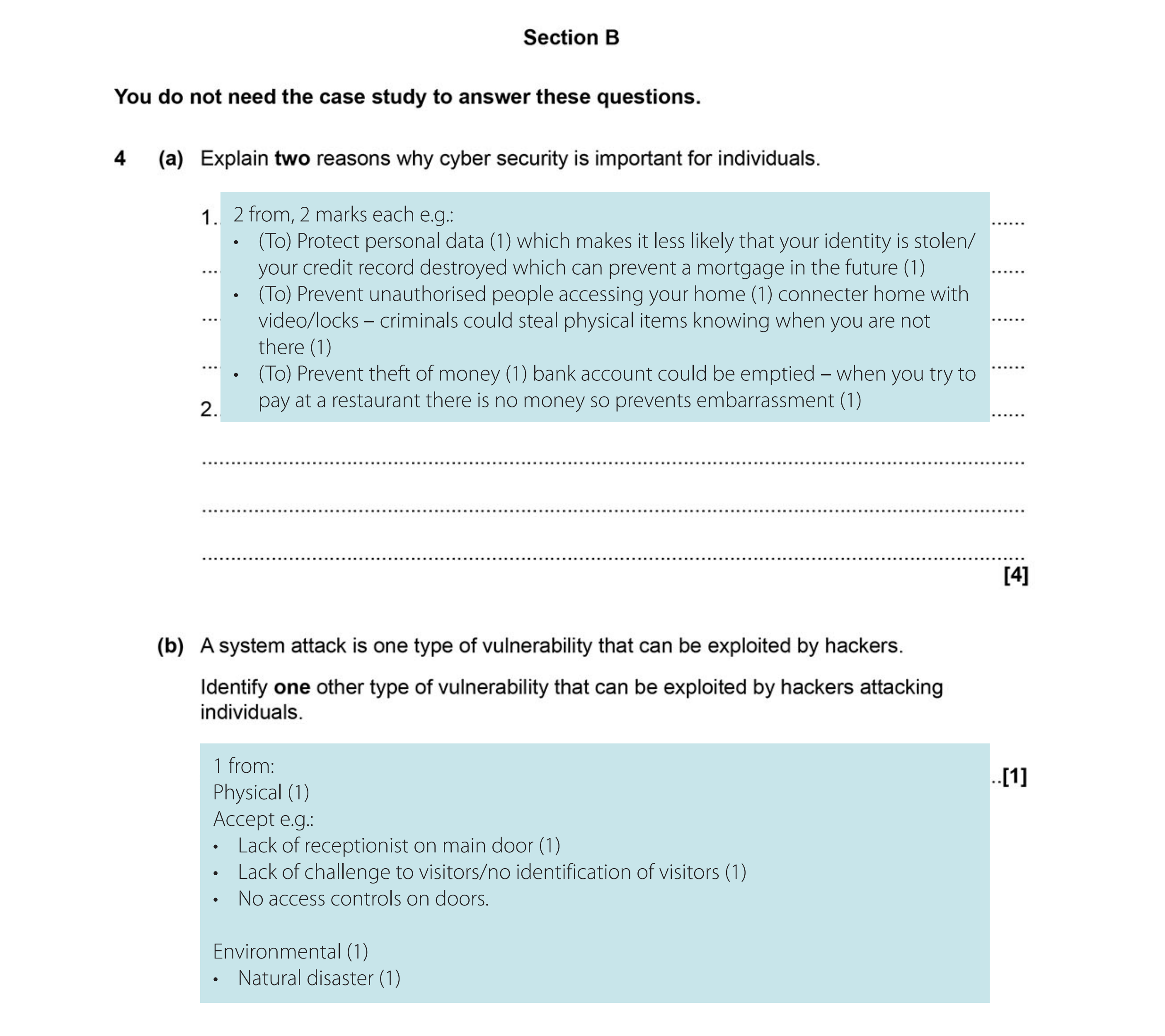
Limited use of examples.

0 marks – Nothing worthy of credit.

Examiner comments

For question 3c, many candidates were fully aware of what a cyber-security incident report was and were able to describe the impact on future incidents. However, whilst a large proportion of candidates wrote answers that were of MB2 standard, few gave really flowing answers that showed a full understanding. This is suggested as an area on which centres could focus for future series.

Questions 4(a) and (b)



Section B

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

4 **(a)** Explain **two** reasons why cyber security is important for individuals.

1.

2 from, 2 marks each e.g.:

- (To) Protect personal data (1) which makes it less likely that your identity is stolen/ your credit record destroyed which can prevent a mortgage in the future (1)
- (To) Prevent unauthorised people accessing your home (1) connecter home with video/locks – criminals could steal physical items knowing when you are not there (1)
- (To) Prevent theft of money (1) bank account could be emptied – when you try to pay at a restaurant there is no money so prevents embarrassment (1)

2.

[4]

(b) A system attack is one type of vulnerability that can be exploited by hackers.

Identify **one** other type of vulnerability that can be exploited by hackers attacking individuals.

1 from:

Physical (1)

Accept e.g.:

- Lack of receptionist on main door (1)
- Lack of challenge to visitors/no identification of visitors (1)
- No access controls on doors.

Environmental (1)

- Natural disaster (1)

[1]

Mark Scheme Guidance

Question 4(a):

Answers should be in the form of an identified reason (1) plus an explanation of that reason (1).

Can be explained through the use of an example.

Take "personal data" as meaning any data about the individual – this includes name etc, as well as bank details.

Question 4(b):

Not system attack.

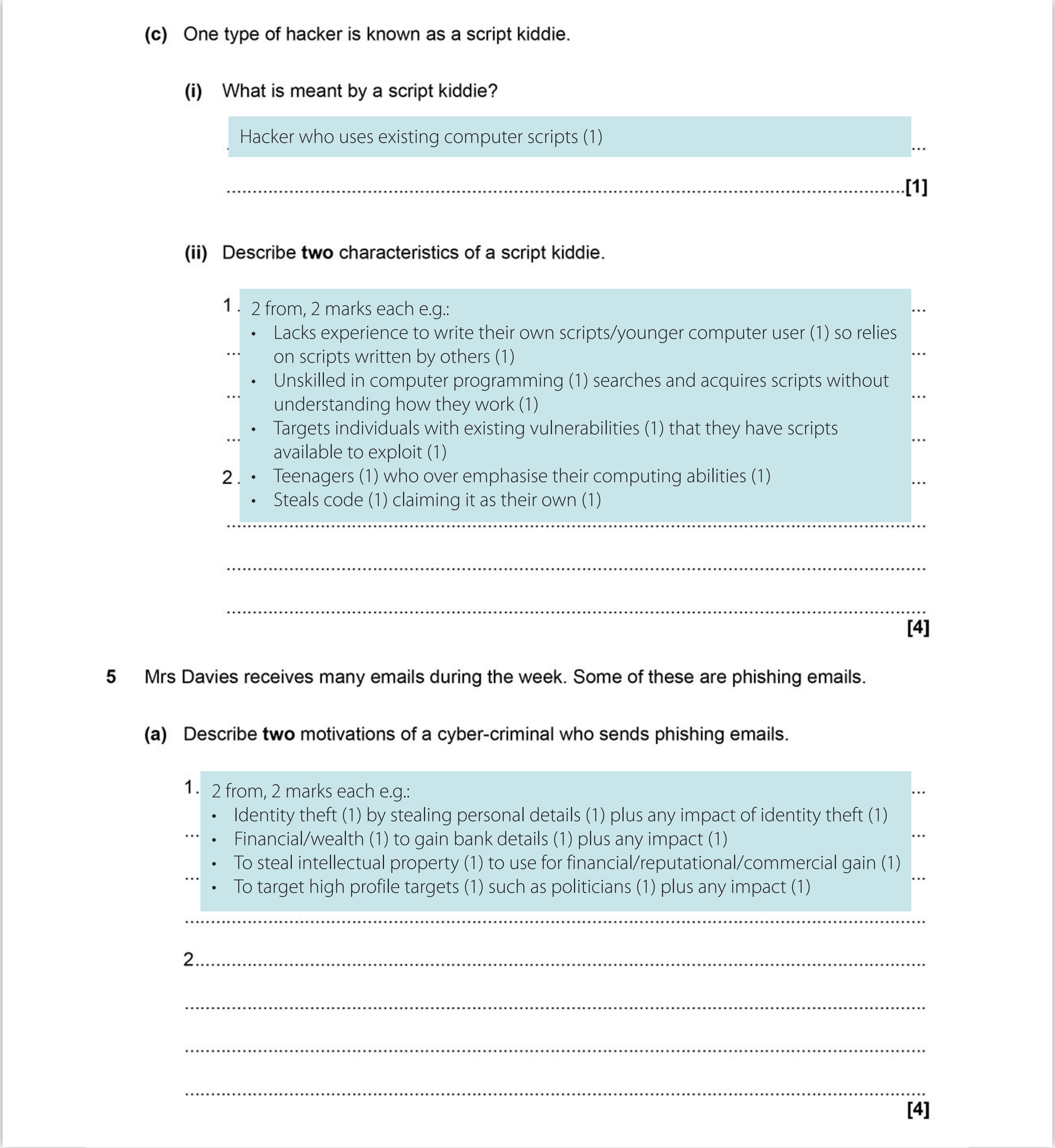
Allow examples of physical and environmental.

Examiner comments

Question 4(a) – When candidates are asked to explain an implication, marks are generally awarded as one mark for identifying the implication and the second mark for explaining why it is significant. With this in mind, many candidates were able to identify an implication (such as details may be lost, or the candidate may suffer from identity theft) but few stated why identity theft was of importance. To continue the focus on identity theft, in order to achieve the full marks for this question, candidates had to give some indication of the impact of identity theft – such as having to contact a bank to check on standing orders or other outgoings, or potential impacts on an individual's credit rating.

Very few candidates were able to give a correct answer for question 4b.

Questions 4(c) and 5(a)



(c) One type of hacker is known as a script kiddie.

(i) What is meant by a script kiddie?

Hacker who uses existing computer scripts (1)

....**[1]**

(ii) Describe **two** characteristics of a script kiddie.

1.

2 from, 2 marks each e.g.:

- Lacks experience to write their own scripts/younger computer user (1) so relies on scripts written by others (1)
- Unskilled in computer programming (1) searches and acquires scripts without understanding how they work (1)
- Targets individuals with existing vulnerabilities (1) that they have scripts available to exploit (1)
- Teenagers (1) who over emphasise their computing abilities (1)
- Steals code (1) claiming it as their own (1)

2.

....**[4]**

5 Mrs Davies receives many emails during the week. Some of these are phishing emails.

(a) Describe **two** motivations of a cyber-criminal who sends phishing emails.

1.

2 from, 2 marks each e.g.:

- Identity theft (1) by stealing personal details (1) plus any impact of identity theft (1)
- Financial/wealth (1) to gain bank details (1) plus any impact (1)
- To steal intellectual property (1) to use for financial/reputational/commercial gain (1)
- To target high profile targets (1) such as politicians (1) plus any impact (1)

2...

....**[4]**

Mark Scheme Guidance

Question 4(c)(i):

Do not mark characteristics.

Question 4(c)(ii):

Must be a characteristic and not just an action.

Question 5(a):

Identification is not required to gain the marks as long as the description has enough detail to know the type of motivation.

Must be a motivation behind the attack. "To get data/information" is not enough.

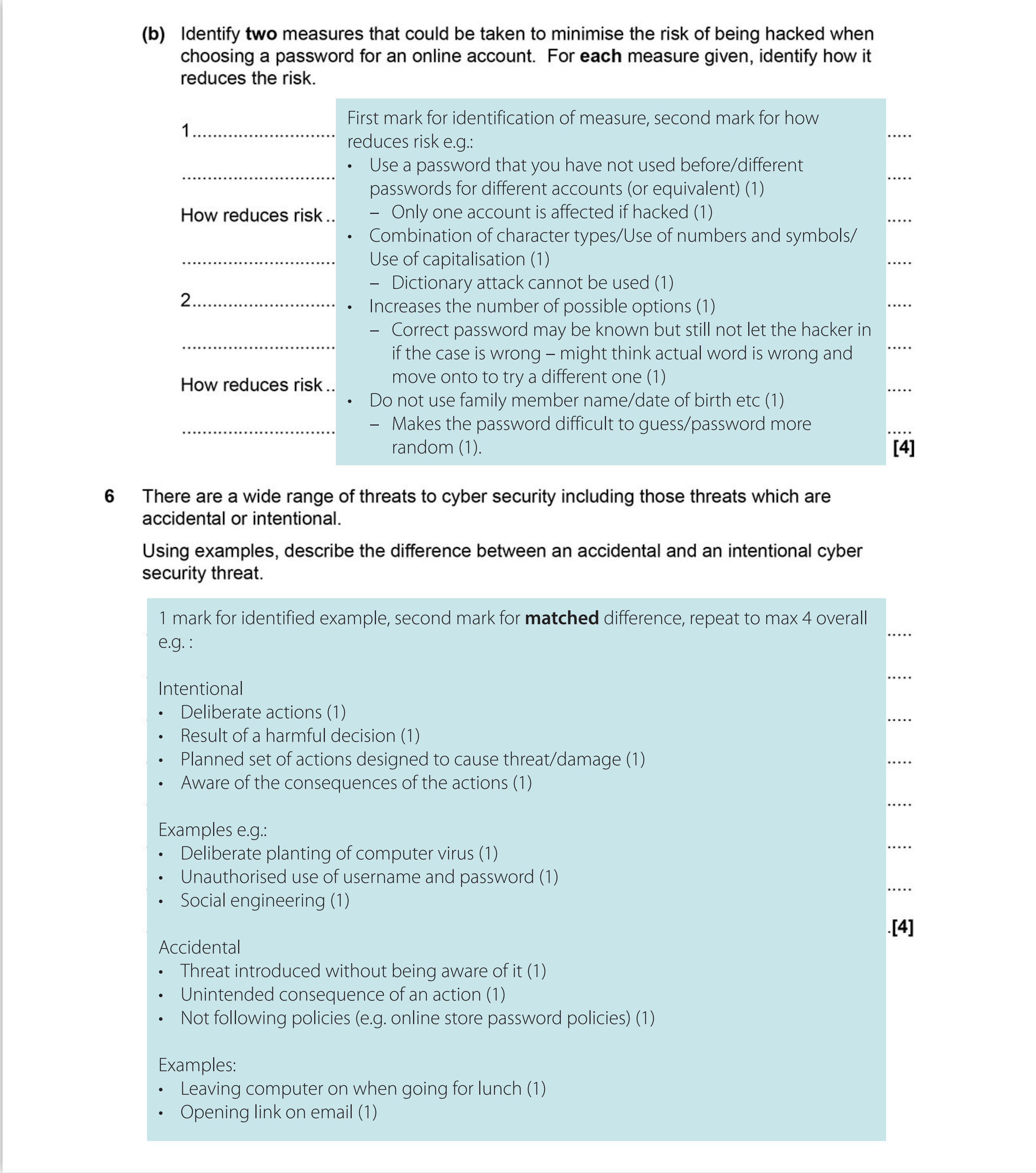
Examiner comments

Question 4(c) – For question 4c, many candidates achieved good marks across the question as a whole. The vast majority were aware that a script kiddie was a person with few actual programming skills, but was more of a dabbler who uses other people's scripts and techniques.

Question 5(a) – The problem with question 5a was that whilst virtually all candidates knew what the term 'phishing' meant, they then struggled with the motivation. Where candidates gave generic answers, such as 'for the thrill of it', these were not accepted.

However, many candidates correctly identified attempts to gain access to personal data, or to gain revenge and so full marks were awarded.

Questions 5(b) and 6



(b) Identify **two** measures that could be taken to minimise the risk of being hacked when choosing a password for an online account. For **each** measure given, identify how it reduces the risk.

1.............................

....

How reduces risk ..

....

2.............................

....

How reduces risk ..

.... **[4]**

First mark for identification of measure, second mark for how reduces risk e.g.:

- Use a password that you have not used before/different passwords for different accounts (or equivalent) (1)
  - – Only one account is affected if hacked (1)
- Combination of character types/Use of numbers and symbols/ Use of capitalisation (1)
  - – Dictionary attack cannot be used (1)
- Increases the number of possible options (1)
  - – Correct password may be known but still not let the hacker in if the case is wrong – might think actual word is wrong and move onto to try a different one (1)
- Do not use family member name/date of birth etc (1)
  - – Makes the password difficult to guess/password more random (1).

6 There are a wide range of threats to cyber security including those threats which are accidental or intentional.

Using examples, describe the difference between an accidental and an intentional cyber security threat.

[4]

1 mark for identified example, second mark for **matched** difference, repeat to max 4 overall e.g. :

Intentional
- Deliberate actions (1)
- Result of a harmful decision (1)
- Planned set of actions designed to cause threat/damage (1)
- Aware of the consequences of the actions (1)

Examples e.g.:
- Deliberate planting of computer virus (1)
- Unauthorised use of username and password (1)
- Social engineering (1)

Accidental
- Threat introduced without being aware of it (1)
- Unintended consequence of an action (1)
- Not following policies (e.g. online store password policies) (1)

Examples:
- Leaving computer on when going for lunch (1)
- Opening link on email (1)

Mark Scheme Guidance

Question 5(b):

Only award answer to do with choosing a password. Do not award answers to do with maintaining security once the password has been chosen.

Only award "password harder to figure out/guess/takes longer to work out password" as expansion once.

Question 6:

1 mark for example of intentional, one mark for example of accidental.

2 marks for differences can be obtained through a single contrasting statement

Mark the whole answer.

The example must be an activity. Stating that the activity is to hack is not enough.

This must be a threat and not a consequence.

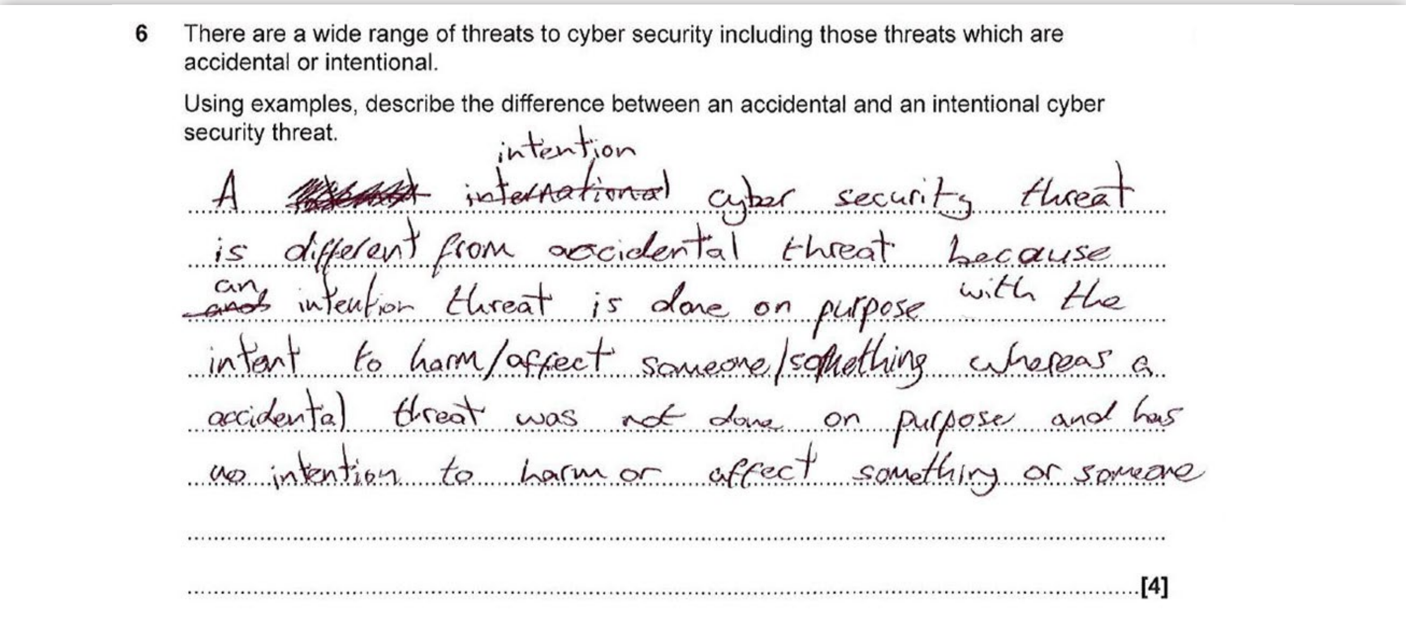
Examiner comments

Question 5(b) – For question 5b, where candidates gave answers that were applicable to the choice of password, the vast majority achieved full marks for this question. Some candidates missed the point of the question and discussed measures such as changing a password regularly and so did not achieve full marks.

Question 6 – Candidates generally did extremely well at this question with most fully aware of the difference between accidental and intentional threats.

Exemplar candidate work

Question 6 – Medium level answer



6 There are a wide range of threats to cyber security including those threats which are accidental or intentional.

Using examples, describe the difference between an accidental and an intentional cyber security threat.

A [illegible] ~~international~~ intention cyber security threat is different from accidental threat because ~~and~~ an intention threat is done on purpose with the intent to harm/affect someone/something whereas a accidental threat was not done on purpose and has no intention to harm or affect something or someone

[4]

Commentary

The question asks for candidates to use examples to describe the difference between the types of security threat. This candidate has not given examples of either intentional or accidental threats other than explaining what an accidental or an intentional threat is. Therefore cannot achieve full marks for this question.

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

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.

OCR acknowledges the use of the following content:
Square down and Square up: alexwhite/Shutterstock.com

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

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

ISO 9001

UKAS MANAGEMENT SYSTEMS 001