Cambridge TECHNICALS LEVEL 3

IT

Combined feedback on the June 2017 exam paper (including selected exemplar candidate answers and commentary)

Unit 3 – Cyber security
Version 1
CONTENTS

Introduction 3
General examiner comments on the paper 4
Pre-release material 5

Section A 7
Question 1 (a) 7
Question 1 (b) (i) 7
Question 1 (b) (ii) 8
Question 2 (a) 9
   Exemplar candidate work with commentary 10
Question 2 (b) 15
Question 3 (a) 16
Question 3 (b) 17
Question 3 (c) 18
Question 4 19
   Exemplar candidate work with commentary 20

Section B 24
Question 5 (a) 24
   Exemplar candidate work with commentary 25
Question 5 (b) 28
Question 5 (c) 29
Question 6 (a) 30
Question 6 (b) 31
Question 6 (c) 32
INTRODUCTION
This resource brings together the questions from the June 2017 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 2a, 4 and 5a.

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
GENERAL EXAMINER COMMENTS ON THE PAPER

Compared to the January examination series for this qualification, candidates were far more prepared and, consequently, able to answer the questions. As a result, more candidates will have accessed the higher grades for the paper.

Whilst there should be celebration of this improved preparation, many candidates are still not answering the question that has been set. For example, question 2(a) asked candidates to reflect on the impact of a Data Security breach on candidates. Many candidates preferred to concentrate on the impact on the hotel, and so did not score marks. Similarly, candidates are not differentiating between questions where they are expected to describe an impact and ones where they have to explain. This lack of understanding means that, in many cases, the extension given to an answer is irrelevant.

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
OCR Hotels

OCR Hotels is an organisation that runs a chain of hotels in Worcester. OCR Hotels provides services to individuals and companies. Each hotel is made up of different areas: • guest bedrooms; • conference centre; • restaurant; • coffee shop.

OCR Hotels is owned by a consortium of shareholders.

IT facilities

WiFi facilities are provided throughout each hotel. In public areas such as the restaurant and coffee shop, access is provided by an open WiFi network and is free of charge. In the guest rooms, WiFi is encrypted and access is obtained by entering a pass code which is received during check in. A wired connection is also available.

Each conference centre also has WiFi facilities for the delegates and each booking has a different access code. There is also a WiFi connection protected by a separate access code for staff use throughout each hotel.

Fig. 1 shows the current network availability in the hotels.

---

**Fig. 1**

- **Guest Rooms**
  - Wired connection
  - WiFi connection (with passcode)

- **Conference Centre**
  - WiFi connection (with passcode)

- **Public Areas (open WiFi network)**
  - Restaurant
  - Coffee shop

- **Throughout Hotel**
  - WiFi connection (with passcode) for staff use

---

Internet
OCR Hotels uses a variety of different centralised systems including:
- booking;
- personnel;
- stock control;
- stock ordering;
- invoicing;
- customer management.

OCR Hotels offers customers the ability to book its facilities via telephone or using online booking services through its website. The online booking services on the website allows customers to create an account and store payment information against their account to simplify the process of payment, making it quicker and easier for the guests. OCR Hotels has recently launched an app which also allows customers to check their bookings and pay any outstanding invoices.

Cyber Security Team

OCR Hotels has noticed an increase in the number of attempted hacks against its computer system and so has set up a cyber security team whose primary role is to detect and prevent any intrusions into the computer system. The team also has responsibility for ensuring the availability of the computer systems and the protection of data stored in them.

The Cyber Security Team logs each attempted intrusion using a formal reporting template and this is used to improve security of the system. It is also used to train employees. After each attempted intrusion, the Cyber Security Team will make recommendations on changes to procedures, hardware/software controls or training required to prevent similar attacks in the future.

The Cyber Security Team makes use of third party companies on a regular basis to test its security procedures and ensure the systems are protected.

Further research

To prepare for the examination, you should carry out research into the following themes:
- The impacts of cyber security incidents on the hotel and its stakeholders.
- The benefits, drawbacks and implications of employing ethical hackers.
- The motivations that drive hackers and the different areas within an organisation that they may target.
- The importance and purpose of incident reports.
Section A

Answer all the questions.

1 (a) The aims of cyber security include protecting information and making it available.

Using an example related to OCR Hotels, describe what is meant by the term availability within the context of cyber security.

Two marks, one for example e.g.

- Information is accessible when required (1) e.g. booking information on customers when they book in (1)
- Only accessible to authorised viewer (1) e.g. only receptionists can see credit card details of customers. (1)
- How easy it is for a person to access the data you need (1) such as front desk staff checking bookings (1)

Mark Scheme Guidance

If no example then max 1 mark.

(b) One target for cyber security threats are the customers of OCR Hotels.

(i) Explain one reason why a hacker might want to gain access to OCR Hotels customer data.

Two from e.g.

- So they know when they are at the hotel (1) so they can rob the house (1)
- So they can gain access to their card/bank details (1) and steal money (1)
- Can use information for criminal activities (1) such as identity theft (1)

Mark Scheme Guidance

The answer needs to be more than the information they would gain but why they would want it.

Examiner comments

Parts (a) and (b) were well dealt with, although candidates from across the ability range failed to give an example for Question 1(a), as required. Similarly, whilst virtually all candidates were able to state a reason why a hacker might want to gain access to customer data, the number who actually explained why this would be done was relatively few.
(ii) Identify one other target for cyber security threats at OCR Hotels. For your chosen target, identify information that could be gained from them and explain how it could be used by a hacker.

Target ........................................................................................................................................

Information gained ......................................................................................................................

Four marks. e.g.

• Staff (1) credit card details (1) used to impersonate an individual (1) and steal money (1)

• Web host (1) credit card details (1) used to impersonate an individual (1) and steal money (1)

• Suppliers (1) identity of delivery drivers (1) to know who to impersonate (1) to gain physical access to the hotel (1)

• Equipment (1) passwords (1) to gain access to computer system (1) to steal address details (1)

Mark Scheme Guidance

The identified target must have something to do with the hotel.

Do not allow customers.

Target must be within the hotel, not the hotel itself.

Target and use must be linked.

Examiner comments

Part b(ii) was misinterpreted by many candidates. The focus of the question was on targets at OCR Hotels, rather than the hotel itself. Where candidates talked about individuals, or systems, such as the Wi-Fi network, this was acceptable, but answers about the Hotel and its fundamental functions were not accessible.
2 OCR Hotels has suffered a cyber security attack which has resulted in the theft of customer data.

(a) Discuss possible impacts of the cyber security incident involving the theft of customer data on the customers of OCR Hotels.

Indicative content:
- They might try and spend on their credit cards but find that there is not credit – might not be able to purchase the items/have to return them – leads to embarrassment.
- Identity theft – their details can be stolen and someone can impersonate them, running up debts, destroying credit history and making it difficult for them to buy items/mortgages in the future.
- The location is known on certain dates which means that they are not at home which will be empty so hackers can arrange for it to be broken into.

Mark Scheme Guidance

Level of response marking:

7 - 10 marks
Candidate has shown a detailed level of understanding by discussing impacts on the customers. 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.

4 – 6 marks
Candidate has shown a good level of understanding by explaining at least one impact on the customers. Some examples will be used to support the explanation which may not be relevant and may at times detract from fluency of narrative. At the bottom end of the mark band, the candidate may have described a single impact. There is a line of reasoning presented with some structure. The information presented is in the most part relevant and supported by some evidence.

1 – 3 marks
Candidate has identified points relevant to impacts of the theft of customer data. Limited use of examples to accompany the description and ideas will be poorly expressed. At the bottom end of the mark band, a single impact may be identified with an example. The information is basic and 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

As mentioned above, many candidates missed the focus of this question and described impacts on the Hotel. Whilst it was sometimes possible to pick out small areas where such answers dealt with customers, these answers usually only resulted in a few marks being awarded.

Where candidates focussed on the correct element, answers were generally good, although very few candidates wrote answers that showed real clarity of answers.

As the question did not specify internal or external stakeholders, markers accepted answers that dealt with stakeholders in the widest sense. However, even with this provision, some candidates pushed the boundaries of acceptable answers and so achieved no marks. For example, the Government would be, at best, a very indirect stakeholder for OCR Hotels. This question was well answered in the main, with many candidates able to clearly identify and explain an impact.
Exemplar candidate work

Question 2(a) – Low level answer

There are lots of possible impacts of the cyber security incident involving the theft of customer data on the customers and our hotel.

The first possible impact would be that they would lose their reputation amongst customers, because customers would be unhappy as they would have lost their personal/financial data. This could lead to them losing their money or losing their identity. This could mean that the hotel could easily earn from their name which would mean that they have to pay it back and be derided from the system. This would decrease our hotel's reputation as it will not be trusted in the money which fewer less customers will come, this will decrease the profit revenue and the profit margin would decline.

Another possible impact would be that they would have even more financial losses. As the customers could sue them under the Data Protection Act (DPA) 1998, the hotel would have followed the 8 principles. This would mean that they will have a sufficient loss and could be taken to court which will decrease their brand loyalty even further.
Commentary

The candidate is directed to consider the impacts of a cyber security incident on customers of the hotel. The candidate has considered the impact on the hotel itself for the whole of the question. However, one mark has been awarded as the candidate has identified that the customer could follow up the incident under the Data Protection Act. This has been taken as an impact.

In order to improve this to a medium level answer, the candidate needed to have focussed on the impact of the cyber security incident on customers, rather than the hotel, and have explained that impact.
Exemplar candidate work
Question 2(a) – Medium level answer

Commentary

This answer focuses on the impact of the cyber security incident on customers, although it does include some impacts on the hotel itself. However, marks have been awarded positively, and there has been no negative impact on the marks awarded.

The answer has examples of impacts and is, in the main, a list, along with some examples. Candidates may be awarded a mark from the bottom end of MB2 where they have described at least one impact. As the candidate has identified and exemplified numerous issues, this work was treated as having just met the criteria for the bottom end of MB2.

In order to improve this work, the candidate needs to expand upon the answers given. For a more secure mark within MB2, there needs to be an explanation of at least one of the issues identified, whilst for MB3, the work will be in significantly more depth than that presented here. For MB3, there should be a full discussion of a range of different issues, with clear use of examples to support the points being made.
Exemplar candidate work

Question 2(a) – High level answer

Customers may have had financial information about them stolen, meaning an attacker could use these details to pay for things from their credit card or just outright steal the money by transferring it to their own account.

Personal information of customers, if accessed, could be used to commit fraud or identity theft, meaning that the actions of the attacker would be attributed to the customer.

Customers may have to spend considerable time cancelling credit cards and ensuring the security of their financial and personal information, causing inconvenience for the customer.

Personal information such as addresses and phone numbers could be leaked, meaning any professional customers may be victims of harassment as a result of this leak.

An attacker could blackmail any professional customers by threatening to reveal personal information about them, unless they receive payment, causing a lot of stress and possible financial loss for the customer.

Customers would no longer trust OCR hotels and would most likely take their custom somewhere else.

Customers may have to go through a lengthy legal process in order to get...
Commentary

The candidate has identified and then explained a number of different issues. The range of issues covered is wide and there is clear expansion of each of these. The answer itself does not flow as easily as it could and, despite each answer being an explanation of issues, these are not linked into a cohesive overarching answer.

The ability to write a sustained and well-developed answer is a key criteria for extended answers in this paper. The absence of this means that full marks cannot be awarded.

Compensation from OCR likely for damages.

Caused by the leaking of their personal information.
(b) The customers are one stakeholder at OCR Hotels.

Explain the impact of the cyber security incident on **two other** different stakeholders at OCR Hotels.

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shareholders/owners</td>
<td>Share price will fall as there is a lack of confidence as customers will not book in the future</td>
</tr>
<tr>
<td>Employees</td>
<td>May be made redundant as bookings will be cancelled as customers move to a different hotel</td>
</tr>
<tr>
<td>Network manager</td>
<td>May not be able to get another job as his reputation for allowing a cyber security attack may follow him</td>
</tr>
</tbody>
</table>

Two marks for a full explanation of the impact on each stakeholder.

**Mark Scheme Guidance**

Answer is about the impact, not who the stakeholder is. Therefore, stakeholder does NOT have to be mentioned.

Accept **internal and external** stakeholders:

- Suppliers
- Competitors

Accept wider implications, such as reputation impacts and motivation of key staff.

**Examiner comments**

Text to follow.
3 Following the cyber security incident, a report needs to be completed.

(a) The report includes the following sections:

Title
Target

For each of the sections, explain how the information will be used.

Title

Target

Two marks per section:

Title:
• To identify the (focus of the) report (1) to find it for future reference when filed (1)

Target:
• To show what data was targeted/stolen (1) to see if there is a pattern in the targets attacked (1) to identify vulnerabilities that can be prevented/make improvements (1)

Examiner comments

One really surprising outcome of this marking session, was the realisation that very few candidates knew the role of a title for a(i) as a means by which something may be identified and located once filed. Answers in this section, generally, were poor, but this aspect was surprising.

More candidates were able to state how the information on the target could be used, although centres are reminded that candidates should avoid repeating the question as their answer.
(b) Describe two ways the information required for the description of the incident could be gathered.

1. Two marks for each description: e.g.
   - [by examining] Logs (1) detailing ports used (1)
   - Observation / watching on CCTV (1) looking at the route used to gain access (1)
   - Interview/talk to (1) talking to targets of the hack (1)
   - Customer incident reports (1) showing what information was stolen/when the attack occurred (1)
   - Proforma/questionnaire (1) gathers data about the attack (may give examples) (1)

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

Mark Scheme Guidance

Must be a description of a method, with method identified (no method – no mark).

Examiner comments

Section 3(b) of this question suggested that candidates are still weak on technical understanding in this part of the syllabus. Few candidates were able to suggest ways (such as questionnaire, or incidents reports), and instead gave general discussions of what could be done.
(c) **Explain one reason why it is important to complete the section on the impact of the incident in the cyber security incident report.**

Two marks for a full explanation e.g.

- Will identify areas for improvement (1) to prevent the attack happening again (1)
- To allow an action plan to be completed (1) addressing the issues identified (1)
- Those who are affected can be contacted and reassured about the security of their data (1) limiting the implication of the attack (1)
- To understand the extent of the attack (1) so can gauge severity of the attack (1)

**Examiner comments**

For Section 3(c), most candidates were able to state a reason why the impact section should be completed, although relatively few were then able to explain this.
4 OCR Hotels decides to employ an ethical hacker.

Evaluate the implications to OCR Hotels of employing an ethical hacker.

Indicative content:

- Will find the security gaps that can then be closed meaning that “real” hackers will not be able to use them to gain access to OCR Hotel’s computer systems.
- Will enable the Hotel staff to focus on preventing attacks rather than having to learn new skills to try and gain access themselves.
- Ethical hacker may find gaps in security that they do not notify the hotel about and use/sell them to other people to utilise.
- May be seen as a negative move by customers or shareholders as may mean that they think they are vulnerable.

Mark Scheme Guidance

<table>
<thead>
<tr>
<th>Marks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5-7</td>
<td>Candidate has shown a detailed level of understanding and has evaluated the implications to OCR Hotels in detail. Relevant examples will be used to support discussion and ideas will be expressed fluently.</td>
</tr>
<tr>
<td>3-4</td>
<td>Candidate has shown a good level of understanding and has explained the implications to OCR hotels, although the explanations may be one sided. Examples will be used to support explanations which may not be relevant and may at times detract from the fluency of the narrative. At the bottom end of the mark band, the candidate may have described a single implication.</td>
</tr>
<tr>
<td>1-2</td>
<td>Candidate has identified implications to OCR Hotels. There will be limited (if any) use of examples to accompany the points made and ideas will be poorly expressed. At the bottom end of the mark band, a single point may be identified.</td>
</tr>
<tr>
<td>0</td>
<td>Nothing worthy of credit.</td>
</tr>
</tbody>
</table>

Examiner comments

Many candidates understood that an ethical hacker had the skills, and possibly the inclination, to change from being a white hat hacker to a black hat hacker and then extrapolate the impacts from this. However, hardly any attempted to evaluate these implications, other than to give a vague description of a negative or positive impact.
Exemplar candidate work

Question 4(a) – Low level answer

One implication to OCR Hotels of employing an ethical hacker is the trustworthiness of the hacker. This means that if OCR Hotels needs to find employs the ethical hacker they need to know whether if they are a trustworthy hacker to detect any flaws within the system.

Another implication to OCR Hotels of employing an ethical hacker is that they may damage the reputation of the business. This means that OCR Hotels needs to think about employing an ethical hacker whether if they are desperate to hire one or not so therefore if they are taking a risk of employing an ethical hacker they need to consider about the reputation of the business.

Commentary

This candidate has identified trustworthiness and the impact on reputation as two issues. There is minimal expansion of either issue, with the candidate basically repeating the identification with a small amount of extra detail, some of which is irrelevant. The overall quality of expression is weak.

The candidate's answer lacks structure.

This answer has the basics of a good answer. Had the candidate explained why trustworthiness was an issue, by exploring the agenda of an ethical hacker, or had they considered how the reputation could be damaged and why this may be a bad thing, a mark from MB2 could easily have been achieved.
Exemplar candidate work

Question 4(a) – Medium level answer

There could be implications to the hotel of employing unethical hackers.

The first implication is that they will know the knowledge of the computer system and the weaknesses and the vulnerabilities. The implication could be that they could sell the information for financial gain to hackers or other hotels close to their reputation.

Second implication is that the ethical hacker will have seen their bank financial personal details so he could steal the information online or give it to their companies. The implication could be that their companies would have an advantage in they would know one of their rival hotel's financial limiting.

Another implication could be that the ethical hacker might not have been interested in didn’t (go to additional answer & space) please!
Commentary

This answer is marked both on the quality of the content and the fluency of the answer.

The work here includes two unlinked points, with a third weak answer. The points are one sided (concentrating on negative implications only), but do include some examples. The answers can be considered explanations, as they do highlight implications and then develop the answers to explain these. However, these are weak explanations.

The reason why this was not given full marks at MB2 was the lack of coherence in the work and the weakness of the explanations.

In order for this answer to be a high level answer, the candidate needed to have included both sides of the argument, explained the points and come to an evaluative conclusion. The answer would also need to be well written and have fluency.
Exemplar candidate work

Question 4(a) – High level answer

By employing a ethical hacker the hotel is ensuring that they are getting a professional with the correct skillset to fix and find holes in their security. This is beneficial as the hacker will notify the hotel of any flaws they find so they can be fixed. Employing good ethical hackers can be expensive but it also means they will use tactics such as social engineering to find flaws. Ethical hackers will need to have full control of the hotel’s computer system or else hiring one isn’t as effective as they cannot test the entire system for flaws. This means that they will have access to all the data on the system. That is the main disadvantage as the hotel has the possibility to commit a cyber crime. For example the hacker could see future plans for the hotel such as expansion plans and sell them to a competitor. It also the hacker could place malware on the system, or leave a flaw for themselves to gain access at a later date. The board of shareholders will need to consider the complaints by employees and customers that do not want an ethical hacker looking at their details stored on the system. Personally, I believe that hiring ethical hackers is a good thing as there is more cyber crime nowadays and it is better to fix the problem before an incident occurs.

Commentary

This piece of work is clearly of the highest standard. The candidate is clearly fully aware of what an ethical hacker is, and has explained both positive and negative impacts. The work flows really well and comes to a logical conclusion based on the arguments.
Section B

5 Companies offer intrusion testing to see if a network is vulnerable.

(a) Describe two different intrusion tests a company could use to identify potential vulnerabilities in a network.

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

Two from, two marks each, e.g.

- Black box/blind testing (1) where the tester is not given any information about the workings of the system (1)
- Firewall configuration testing (1) checking the settings on the firewall/different to default/set correctly (1)
- Social engineering (1) phoning employees to try and gain passwords (1)

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

Mark Scheme Guidance

Allow generic answers based on internal/external/blind/double blind/black box/white box. Grey box testing as well as specific examples of individual tests..

Examiner comments

This question again suggested a lack of technical understanding, with few candidates able to state an intrusion test, and very few able to describe one. Many candidates gave intrusion detection systems as an answer and missed the fundamental focus of the question.
Exemplar candidate work

Question 5(a) – Low level answer

Commentary

This candidate has included two separate answers. The second, Denial of Service attack, was not accepted as an answer.

The first answer is a vague description of sending a virus. This has been treated as an example of testing the firewall.

In order to improve this to a medium level answer, the candidate would either need to give two suitable answers for what is meant by intrusion testing OR make the first answer more specific. As this answer stands, it is a vague answer that is lacking detail.
Exemplar candidate work

Question 5(a) – Medium level answer

Commentary
In this answer, the candidate has again stated a denial of service attack as their first answer, for which they have not received any marks.
The second answer is a good description of a brute force attack and so 2 marks have been awarded.
In order to improve this answer, the candidate needed to have correctly identified a further suitable example of an intrusion attack.
Candidate style answer

Question 5(a) – High level answer

1. They could use a Brute Force attack. This is where repeated attacks are tried to see if the security can deal with repeated attacks on it.
2. They could use social engineering, which is where someone tries to persuade a friend to let them onto a network.

Commentary

This answer identifies two types of intrusion tests and then describes what each is.
(b) Explain two reasons why an individual should employ a company to conduct intrusion testing of their network.

1 Up to three marks for each answer:
   First mark – Reason
   Second and third mark – explanation of reason
   e.g.
   • They are highly trained at what they do/more skills than the individual (first)
   • Will do a better job than the individual (1) because more likely to identify issues (1)

2 Answer may also be about outcome the tests and why these outcomes occur
   • The company will be able to test for weak points in the network (1) (first)
   • And report these back to the individual (1) so that they can be rectified (1)

Mark Scheme Guidance

Answer may also be about outcome the tests and why these outcomes occur.

Examiner comments

Many candidates were able to give a good answer about why a company should be employed. Answers included the absence of bias, or the benefit of looking at something with a fresh pair of eyes, whilst others compared the likely relative skill levels between a company and an individual. However, few candidates gave a second answer, or, if they did, this was effectively a repeat of the first answer.
(c) Identify two different hardware security controls that the company could implement to protect its network. For each control, describe how it can protect the network.

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

How it protects ........................................................................................................................

- Biometric access (1) coded to an individual (1) hard to duplicate/which are unique (1)

- Alarm (1) notifies others of an intrusion (attempt) (1) so that the break in can be investigated (1)

- Cable locks (1) prevent the computer from being physically removed (1) by attaching it to a fixed item (1)

- Safe (1) prevents access to the data (1) different set of skills required to access data in the safe (1)

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

How it protects ........................................................................................................................

........................................................................................................................................

........................................................................................................................................

........................................................................................................................................

........................................................................................................................................

[6]

Mark Scheme Guidance

Answer MUST be about the security control and NOT the implication.

Examiner comments

As with part A of this question, section C suggested a lack of technical understanding. For those candidates who realised that a hardware control was a form of security other than software, many scored well here, although they sometimes lacked a full description. However, others focussed on software controls, or, apparently guessed at the answer.
6 One possible motivation for a cyber security attack is for the attacker to generate income for themselves.

(a) Identify two ways that a cyber security attack on an individual could be used to generate income by the attacker.

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

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

Mark Scheme Guidance

“Steal personal details” on its own is too vague.

However, if candidate identifies two items of personal data which together could enable identity to be stolen, award identity theft mark point.

Examiner comments

This section required candidates to state how income could be generated. Many candidates understood the general gist of the question, but, having talked about accessing data, for example, then failed to complete the circle by making the point about how income could be generated.

Two from e.g.

- Stealing credit card details/credit card details (1)
- Selling the data on (1)
- Identify theft (1)
- Ransomware (1)
(b) One cyber security control that could be implemented to protect data stored on an individual’s computer is cryptography.

What is meant by the term cryptography?

[ ] One from:

- Storing data in a form that only those with a key can read and process it (1)
- Use of encryption and decryption to prevent data from being understood if intercepted (1)

Examiner comments

A very few candidates were able to give a good description of cryptography in this section.
(c) One consequence of a cyber security attack could be that the data is now inaccessible to the individual. One way that this could be done is by the hacker using cryptography.

Identify two other ways that a hacker could make the data inaccessible.

1 ............................
2 ............................

One from: e.g.
• Delete the data (1)
• Physically breaking the computer/hard drive (1)
• Change passwords (1)
• Move data (1)

Mark Scheme Guidance

DO NOT accept “copy data”
DO NOT accept “encryption”

Examiner comments

Similarly, many candidates stated that encryption was a method of making data inaccessible. This answer had been specifically excluded by the reference to cryptography in the question.
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

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.

© OCR 2017 Oxford Cambridge and RSA Examinations is a Company Limited by Guarantee. Registered in England. Registered office 1 Hills Road, Cambridge CB1 2EU. Registered company number 3484466. OCR is an exempt charity.