# CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>General examiner comments on the paper</td>
<td>4</td>
</tr>
<tr>
<td>Case Study</td>
<td>5</td>
</tr>
<tr>
<td>Section A</td>
<td>6</td>
</tr>
<tr>
<td>Question 1 (a)</td>
<td>6</td>
</tr>
<tr>
<td>Question 1 (b))</td>
<td>6</td>
</tr>
<tr>
<td>Question 1 (c)</td>
<td>6</td>
</tr>
<tr>
<td>Question 1 (d)</td>
<td>7</td>
</tr>
<tr>
<td>Question 1 (e) (i)</td>
<td>7</td>
</tr>
<tr>
<td>Question 1 (e) (ii)</td>
<td>7</td>
</tr>
<tr>
<td>Question 1 (e) (iii)</td>
<td>8</td>
</tr>
<tr>
<td>Question 2 (a) (i)</td>
<td>10</td>
</tr>
<tr>
<td>Question 2 (a) (ii)</td>
<td>10</td>
</tr>
<tr>
<td>Question 2 (b)</td>
<td>10</td>
</tr>
<tr>
<td>Question 2 (c)</td>
<td>11</td>
</tr>
<tr>
<td>Question 3</td>
<td>13</td>
</tr>
<tr>
<td>Section B</td>
<td>15</td>
</tr>
<tr>
<td>Question 4</td>
<td>15</td>
</tr>
<tr>
<td>Question 5 (a)</td>
<td>16</td>
</tr>
<tr>
<td>Question 5 (b)</td>
<td>16</td>
</tr>
<tr>
<td>Question 6</td>
<td>18</td>
</tr>
</tbody>
</table>
INTRODUCTION

This resource brings together the questions from the June 2016 examined unit (Unit 3), the marking guidance, the examiners comments and the exemplar answers into one place for easy reference.

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/
GENERAL EXAMINER COMMENTS ON THE PAPER

This course, in its current format, was launched for first teaching in September 2016. Therefore, candidates who took this examination did so after approximately four months of teaching. In many cases, this appears to have led to a lack of understanding in depth, with some answers being approached almost as if they were general knowledge questions. Unfortunately, the paper identified significant knowledge gaps across the cohort. Centres are reminded that questions may be drawn from across the specification and that candidates need to be test ready before they are entered. As well as the text book, centres need to draw from other resources, in order to ensure that the specification is covered in sufficient breadth and depth.

The paper is a technical paper that requires an understanding of technical terms. For example, the term ‘hacker’ has a specific meaning within the specification. Candidates should ensure that they have the necessary technical understanding from across the breadth of the specification to ensure that such technical terms are not only recognised, but understood.

In many cases, candidates appeared to have made little use of the case study and associated tasks, in their preparation. However, section B, where no context was applied, really did highlight the lack of depth and breadth of understanding.

Resources which might help address the examiner comments:

From the link below, you’ll find ‘The OCR guide to research’ (along with many other skills guides)

http://www.ocr.org.uk/i-want-to/skills-guides/
CASE STUDY

Organisational profile
The Dependable Banking Group

The Dependable Banking Group provides banking services to private and corporate customers. The Headquarters are in London, but the Group has customers from across Europe. In day-to-day activities, the group uses the name ‘Dependable’ rather than its full official title.

Technology services

Dependable launched both a telephone and an internet banking service in June 2004. Both services allow customers to log onto their accounts and manage standing orders and direct debits, transfer funds and make payments. Dependable also provides other services such as allowing private customers to register mobile phones and other high value items that are then covered by insurance provided by the Banking Group.

Dependable prides itself on its ability to keep at the forefront of the use of technology. Shortly after launching the internet banking service, Dependable launched an App that includes most of the tools found on the main internet banking website. This App is available for all mobile platforms. The App includes a facility that allows customers to request notifications when key events occur on their account. Dependable has also developed a social media presence, but this is currently limited to providing information rather than allowing customers to make payments or use their accounts in other ways. Dependable is currently researching into the use of social media as a platform from which customers will be able to access their accounts in the same way as they are currently able to using the App.

Cyber security team

When Dependable set up its internet banking service, it also set up a cyber security team. This team has two main roles. The first of these roles is customer education and the second is investigation of cyber security breaches.

The customer education role involves the cyber security team providing literature, adverts and web content that warns customers of the threats to their online security. The cyber security team has recently created a Data Protection policy that sets out how Dependable protects the private data and information of all customers. Each customer has been sent a copy of this policy, along with further information on ways in which they can protect their own data on their personal computers and other devices.

The investigation role requires the cyber security team to follow up reported incidents of cyber security breaches. A cyber security incident report is created for each incident the group researches.

Since the launch of the cyber security team, there has been a year-on-year increase in the incidents of attempted and successful cyber security attacks by both hackers and phishers.

Customer experience

Humphrey has recently set up a bank account with Dependable. When he did so, he opted to be able to use both telephone and internet banking. He has been supplied with a user ID and a password to use when he logs on to his account from the internet, but has been told that when he uses telephone banking, he must supply numbers from an eight figure security code, as well as answer questions based on details of his account.

Humphrey is in the final stages of buying a house and is about to receive funds from a mortgage company. This mortgage is not with Dependable, but he has set up a Dependable current and savings accounts to store money that he will use to purchase his house. He has asked that the mortgage funds be paid into his Dependable current account so that he can then combine his funds and complete the purchase of his house.

Further research

To prepare for the examination, you should carry out research into the following themes:

• The use of online and telephone banking.

• Reasons why personal data may be targeted, the methods of doing so and the responses taken by private individuals and organisations to the targeting of data.

• The importance and purpose of policies, procedures and documentation (both internal and external) when dealing with cyber security issues.

• The benefits, drawbacks and implications of allowing access to bank accounts by digital means.
Section A

1 Customers of The Dependable Banking Group (Dependable) have reported attempts to gain unauthorised access to their accounts.

(a) Identify and describe two different methods a hacker could use to gain unauthorised access to customer data.

1. Remote administration programme (1st) that is installed on the user’s computer (1) so that the computer can be controlled by a third party (1).
2. Writing mobile code/java/javascript/activex code (1st) to track which websites are visited (1) on a smartphone (1).

   Any other valid suggestion.

(b) Identify two items of data that would be useful to a hacker who wanted to access Humphrey’s account by telephone banking.

1. Number of standing orders (1).
2. Date of last cash withdrawal (1).

   Any other valid suggestion.

(c) One possible outcome of a cyber security attack is the total loss of data.

   Describe one impact on Humphrey if all data held about him by his bank was lost.

   e.g.

   The bank will not be able to verify who he is (1) and so he may not be able to access his accounts (1).
   His home details will be lost (1) and so he will not receive statements/replaced cards, etc (1).

   Any other suitable implication (1) plus explanation (1).
The cyber security team produces a cyber security incident report after investigating the attempted attacks.

(d) Explain why the attack on Humphrey’s account is more likely to have been done by an individual rather than a government.

- Individual hacker more likely to be after money (1).
- So will target lots of individual accounts (1).
- Government unlikely to be interested in financial details (1).
- Small scale attack for individual/large scale attack for Government (1).
- Any other valid suggestion.

When a customer reports an attempted attack, a set procedure is followed.

(e) Explain why each of the responses below are important to the customer.

(i) Each member of the research team knows their role.

- The team is more likely to solve the case (1) and so reassure the customer (1).
- React to attack faster (1) to be more prepared for next attack (1).
- Any other valid suggestion

(ii) The person completing the report knows which procedure to follow when carrying out the research.

- So that every stage is followed so that the correct people are informed (1) which improves the chances of success (1).
- Customers can have confidence that the procedures for dealing with the attack (1) ensure that all aspects of the attack will be fully and correctly investigated (1).
- The procedures may be industry/banking standards (1) so all attacks are investigated in the same robust way (1).
- Any other valid suggestion.

(iii) Liaising with them throughout the process.

- So that the customer is kept informed (1) and so is less worried/is able to add more information (1).
- Good customer service (1) as the customer feels that they are part of the process (1).
- Any other valid suggestion.
Mark Scheme Guidance

1 (a)
Points marking approach.
Six marks for two full descriptions. MAX mark three per set of answers.
First mark for the correct identification, plus two additional marks for valid description.
Methods must relate to hacker and the use of their technical skills.
DNA phishing, social engineering, guessing, etc.

1 (b)
For two marks.
The identified data must be of use to access personal data by telephone banking.
Scenario states that data will be taken from details of Humphrey's account.

1 (c)
Points marking approach.
Up to two marks for any suitable implication. First mark for identification of impact, 2nd for expansion.
Data loss i.e. there is no data. Focus of this question is on data loss not data theft.

1 (d)
Points marking approach.
Up to three marks for a full explanation.

1 (e) (i)
Points marking approach.
Two marks for a full explanation.
Answer must be in context of importance to the customer.
Accept converse arguments about what happens if stage is not followed.
1 (e) (ii)

Points marking approach.
Two marks for a full explanation.

Answer must be in context of importance to the customer.
Accept converse arguments about what happens if stage is not followed.

1 (e) (iii)

Points marking approach.
Two marks for a full explanation.

Answer must be in context of importance to the customer.
Accept converse arguments about what happens if stage is not followed.

Examiner comments

Question 1 was referred to in the introduction (above). Unfortunately, the vast majority of candidates failed to appreciate that the term ‘hacker’ is not a generic term for someone who attempts to ‘do wrong with computers’ but has a specific meaning. Therefore, the vast majority of answers for Q1a concentrated on phishing or scamming, for example, rather than the use of advanced programming skills to gain unauthorised access to data. Question 1b suffered from a similar problem.

Context is important when answering these questions. For question 1c, candidates were asked to describe one possible impact arising from the total loss of data, held by the bank, about Humphrey. Where candidates realised that this meant the total loss, rather than the ability of one person to access the data, they gave good answers. However, in a significant number of cases, candidates ignored the stem of the question and dealt with the question as though it was a form of identity theft.

Many candidates appreciated that an attack on an individual was more likely to have come from an individual than a government and were able to give good answers to Q1d. However, the wider understanding of the incident reporting procedure, which was the focus of question e (i) to e (iii), was not evident from the answers given. The focus of these questions was on the importance to the customer. In a few cases, candidates were able to deal with this focus. However, in the majority of cases, candidates gave more general answers and ignored any benefit to the customer. Of the three questions, 1e (iii) was the best answered.
2 Humphrey has received a copy of the Data Protection policy from the cyber security team at Dependable.

(a) The Data Protection policy states that data confidentiality is the first priority.

(i) Describe what is meant by the term data confidentiality.

- Access to the data is restricted (1) to those who need access to it/kept away from those who don't need access (1).
- Data which is private / confidential (1) is kept private/confidential (1).
- Data which has increased level of security required (1) to be accessed (1).
- Any other valid suggestion.

(ii) Explain how a breach in data confidentiality could lead to a third party being able to pose as Humphrey.

- Humphrey’s personal data could be used to answer a security question (1) and so allow the 3rd party to pretend to be him (1).
- The 3rd party is able to give private/personal information (1) and so appear to be him (1).
- Any other valid suggestion.

Humphrey has also received an advice pack from the cyber security team.

(b) The advice pack states that Humphrey should encrypt any personal data he holds on his personal computer.

Explain how encryption would protect Humphrey’s personal data.

- If the data is accessed (1) by a 3rd party/hacker (1) then the data is useless to them (1).
- An algorithm is used to scramble the information/plain text (1).
- A code is applied to the data (1).
- Encrypted message/data can only be read if de-encrypted (1).
- Only holders of the encryption key are able to read the message (1).
- Any other valid suggestion.
(c) Humphrey has received an email asking him to confirm his personal details before the mortgage funds are transferred to his account.

Explain two methods that Humphrey could use to check that this email is genuine.

1  ...........................................................................................................
   Contact the mortgage company by phone/fresh email (1) to check that the email has been sent (1).
   Check for spelling errors (1) as phishing emails often have inaccuracies (1).
   Look for personalisation within the email (1) as phishing emails are often very general (1).

2  ...........................................................................................................
   Check that email is from correct the web address/domain name of the mortgage company (1) as phishing emails use similar seeming false addresses (1).
   Any other valid suggestion.

Mark Scheme Guidance

2 (a) (i)
Points marking approach.
Two marks for a full description.
‘Data is kept private’ with no expansion - award one mark only.

2 (a) (ii)
Points marking approach.
Two marks for an explanation of how data (or a named example of data) could be used to impersonate Humphrey.

2 (b)
Points marking approach.
Up to three marks for a full explanation. Read whole answer and mark to candidate’s best advantage.

2 (c)
Points marking approach.
Four marks for two full explanations. MAX mark two per set of answers.
First mark for the correct identification, plus one additional mark for valid explanation.
Examiner comments

Question 2 moved the focus onto the Bank’s Data Protection Policy. The general question about the meaning of ‘data confidentiality’ was dealt with well by most candidates. However, Question 2a(ii), which required candidates to be able to link data confidentiality breaches to how a third party could benefit from that breach, was not as well answered. In a few cases, candidates were awarded two marks, but for most, candidates gave a relatively simple answer that was almost a rewrite of the question and did not consider the implications of holding such personal information.

Question 2b was another question that dealt with the more general question of how encryption works. In most cases, candidates identified this question as one that required a technical explanation and achieved fairly high marks. However, some candidates gave a more descriptive answer that lacked technical understanding.

Question 2c could again be regarded as a question that assessed the candidates’ wider knowledge of cyber security and the quality of answers given reflected the work that many centres have done on this issue over recent years. Most candidates achieved at least two marks for this question, with a sizeable number achieving full marks.
3* Dependable customers have said that they would like to be able to access and manage their accounts from social media platforms.

Discuss the implications to Dependable’s customers if this facility was introduced.

Indicative Content

- Security may be compromised by allowing access directly from Social Media sites.
- Social media sites are outside of the direct control of the Dependable Bank and so may not be as reliable.
- Social media sites may have lower levels of security and so may offer an easier method of access to data.
- Data could be stolen and used for identity theft, with follow on consequences.
- Funds could be transferred from the customer’s account.

Mark Scheme Guidance

Levels of response marking approach

<table>
<thead>
<tr>
<th>Marks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7-10 marks</td>
<td>Candidate has shown a detailed level of understanding by discussing more than one implication for customers if this facility was introduced. Relevant examples will be used to support discussion and ideas will be expressed clearly and fluently. <em>There is a well-developed line of reasoning which is clear and logically structured. The information presented is relevant and substantiated.</em></td>
</tr>
<tr>
<td>4-6 marks</td>
<td>Candidate has shown a good level of understanding by explaining at least one implication for customers if this facility was introduced. Some example(s) 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 of the mark band the candidate may have described a single implication. <em>There will be a line of reasoning presented with some structure. The information presented is the most part relevant and supported by some evidence.</em></td>
</tr>
<tr>
<td>1-3 marks</td>
<td>Candidate has identified point(s) relevant to the introduction of a social media platform on Dependable customers. Limited use of examples to accompany description and ideas will be poorly expressed. At the bottom of the mark band a single point related to the introduction of social media platforms may be identified with an example. <em>The information is basic and is communicated in an unstructured manner. The information is supported by limited evidence and the relationship to the evidence may not be clear.</em></td>
</tr>
<tr>
<td>0 marks</td>
<td>Nothing worthy of credit.</td>
</tr>
</tbody>
</table>
Examiner comments

Question 3 assessed subject knowledge as well as candidates’ use of English. Generally, candidates seemed ill-prepared for this type of question and gave relatively narrow answers that tended to focus on simple and, often, single issues. This tended to be the negative impact of security, but other than this general point, candidates generally failed to expand on their answers and gave relatively poorly developed responses.
## Section B

### 4. Access controls can be used to protect data.

Identify and describe one type of access control other than encryption that can be used to protect the data held by the accounts office of a book retailer.

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical</td>
<td>(1st) an intruder alarm could be placed in the room (1) where the servers are held (1).</td>
</tr>
<tr>
<td>Firewall</td>
<td>(1st) monitors network traffic (1) and controls the flow of data out of the system (1).</td>
</tr>
<tr>
<td>Biometric</td>
<td>(1st)…</td>
</tr>
<tr>
<td>Any other valid suggestion.</td>
<td></td>
</tr>
</tbody>
</table>

---

### Mark Scheme Guidance

Points marking approach.

Up to three marks.

First mark is for identification of a method of Access Control. Second and third marks are for the description of the Access Control method.

If candidate does not identify a form of access control, no marks are to be awarded.

DO NOT award marks for encryption

### Examiner comments

For question 4, most candidates were able to give a good description of access control, with most achieving either 2 or 3 marks.
5 Intrusion Prevention Systems (IPS) can be used to check systems to make sure that they are safe from attack.

(a) Using examples, justify the use of an IPS to analyse the vulnerability of a system used by a school to hold contact details of its students.

<table>
<thead>
<tr>
<th>Indicative Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPS uses real-time tracking and responds to identified attacks to block access to IP addresses.</td>
</tr>
<tr>
<td>Records are kept (audit logs, etc.) so that lessons may be learnt from previous attempts.</td>
</tr>
<tr>
<td>Student records are likely to be a low priority target for attack.</td>
</tr>
<tr>
<td>Most attempts to gain access to data are likely to be by phone-call or other direct contact and so the use of audit trails and incident logs to create pro-forma responses allows staff to follow procedures, based on previous incidents.</td>
</tr>
</tbody>
</table>

(b) One criticism of using IPS is that it reacts rather than protects.

Evaluate this comment with the aid of examples.

| e.g. |
| Protection is the process of stopping an event happening (1). |
| IPS monitor systems and react to them (1). |
| Therefore, IPS systems react after the event (1). |
| Delay in reaction can be very slight (1). |
| Once IP address/ port/threat identified all traffic blocked from there (1). |
| Conclusion based on points made (1). |
| Use of suitable example (1). |
| Any other valid suggestion. |
Mark Scheme Guidance

5 (a)

Levels of response marking approach.

<table>
<thead>
<tr>
<th>Marks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5-7</td>
<td>Candidate has justified the use of IPS to protect pupil data. Justification is based on clear reasoning supported by points explained in the argument, which are in turn supported by examples. Ideas will be expressed clearly and fluently.</td>
</tr>
<tr>
<td>3-4</td>
<td>Candidate has shown a good level of understanding of the use of IPS and has explained this in the context of the protection of pupil data. The supporting argument may be lacking the use of examples, or where examples have been used, these are not used strongly, or the supporting argument may be poorly developed and lacking in detail.</td>
</tr>
<tr>
<td>1-2</td>
<td>Candidate has identified some points relevant to the use of IPS to protect pupil data. There may be some doubt that the candidate fully understands the term IPS. There may be examples, but these are not used as part of a coherent answer.</td>
</tr>
<tr>
<td>0</td>
<td>Nothing worthy of credit.</td>
</tr>
</tbody>
</table>

5 (b)

Up to six marks. If no conclusion, MAX five.

Read whole answer and mark to candidate’s best advantage.

The answer as a whole should be read and conclusion awarded if it is based on the points made.

1 mark may be awarded for an overall statement of the validity of the statement, even if not supported by arguments.

Examiner comments

For question 5a, few candidates appeared to appreciate the nature of an Intrusion Prevention System, and were even less prepared to justify one’s use within the scenario given. The question specifically asked for examples to support any points made and candidates were, again, ill-equipped to provide these. Question 5b followed the theme set by question 5a and asked about the reactive versus proactive nature of an Intrusion Prevention System. Despite a very clear lead within the question, few candidates actually addressed this issue and, instead, gave general answers at best, that only earned a few marks.
6 Scammers and phishers are types of attackers that could be involved in a cyber security attack on a multinational company.

Compare the characteristics of these two types of attackers.

<table>
<thead>
<tr>
<th>Marks</th>
<th>Marking Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 marks</td>
<td>Two complete comparisons</td>
</tr>
<tr>
<td>3 marks</td>
<td>One complete comparison and one individual point</td>
</tr>
<tr>
<td>2 marks</td>
<td>One complete comparison</td>
</tr>
<tr>
<td>1 mark</td>
<td>One individual point about either side</td>
</tr>
</tbody>
</table>

- Scammers send an email with a false link (1) a phisher directs the victim to a false website (1).
- Phishers tend to target many people at the same time (1) whilst a scammer tends to target on an individual basis (1).
- A scammer is cyber-enabled (1) whilst a phisher is cyber-dependant (1).
- Scammers defraud their target/example provided (1) whilst phishers attempt to get personal details example provided which they then use (1).
- Scammers & phishers pretend to be something/ someone/an organisation which they are not (1).
- Any other valid suggestion.

Mark Scheme Guidance

To be awarded comparisons the difference between a scammer and phisher must be clearly defined.

If a clear comparison is provided, then two marks may be awarded. The comparisons may not be consecutive in the answer.

Examiner comments

Question 6 focussed on scammers and phishers. Candidates seemed well prepared for this sort of question and were able to compare the characteristics of these two types of attackers with relative ease and fairly good levels of success.
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.