# Cambridge Technicals
# IT

## Unit 3: Cyber Security

Level 3 Cambridge Technical in IT
**05838 – 05842/05877**

# Mark Scheme for January 2021

OCR (Oxford Cambridge and RSA) is a leading UK awarding body, providing a wide range of qualifications to meet the needs of candidates of all ages and abilities.  OCR qualifications include AS/A Levels, Diplomas, GCSEs, Cambridge Nationals, Cambridge Technicals, Functional Skills, Key Skills, Entry Level qualifications, NVQs and vocational qualifications in areas such as IT, business, languages, teaching/training, administration and secretarial skills.

It is also responsible for developing new specifications to meet national requirements and the needs of students and teachers.  OCR is a not-for-profit organisation; any surplus made is invested back into the establishment to help towards the development of qualifications and support, which keep pace with the changing needs of today’s society.

This mark scheme is published as an aid to teachers and students, to indicate the requirements of the examination. It shows the basis on which marks were awarded by examiners. It does not indicate the details of the discussions which took place at an examiners’ meeting before marking commenced.

All examiners are instructed that alternative correct answers and unexpected approaches in candidates’ scripts must be given marks that fairly reflect the relevant knowledge and skills demonstrated.

Mark schemes should be read in conjunction with the published question papers and the report on the examination.

© OCR 2021

Abbreviations, annotations and conventions used in the detailed Mark Scheme (to include abbreviations and subject-specific conventions).

| Annotation | Meaning |
|---|---|
| / | alternative and acceptable answers for the same marking point |
| ✓ | Separates marking points |
| **DO NOT ALLOW** | Answers which are not worthy of credit |
| **IGNORE** | Statements which are irrelevant |
| **ALLOW** | Answers that can be accepted |
| **( )** | Words which are not essential to gain credit |
| __ | Underlined words must be present in answer to score a mark |
| **ECF** | Error carried forward |
| **AW** | Alternative wording |
| **ORA** | Or reverse argument |

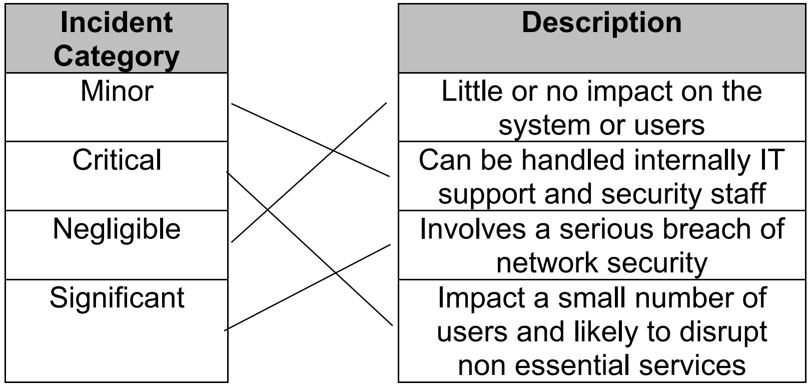
| Question | | | Answer | Marks | Guidance |
|---|---|---|---|---|---|
| **1** | **(a)** | **(i)** | Two from, two marks each, e.g.<br>• Competitive advantage (1) other companies cannot get their research and get a product to the market first (1)<br>• Part of the contract requirements (1) for example a government contract will require security (1)<br>• To allow Stevenson Research to function day to day (1) and to know what they need to do (1)<br>• Data can be used to attack the company (1) e.g. software version being run on switches (1)<br>• If the research data is altered/modified (1) completing the contract could be delayed (1) | 4 | Do not allow answers relating to personal data |
| **1** | **(a)** | **(ii)** | Two from, one mark each:<br>• Personal / Individual (1)<br>• Health (1)<br>• Customer/visitor (1)<br>• Employee (1)<br>• Financial (1)<br>• National insurance (1)<br>• State/Government (1)<br>• Economic (1)<br>• National Security (1)<br>• Technical (1)<br>• Research (1) | 2 | **Do not** accept examples of data |
| **1** | **(b)** | | Two from, two marks each:<br>Environmental e.g.<br>• Naturally occurring (1)<br>• Wildfire/Volcano/etc. (1)<br>Physical e.g.<br>• Theft/vandalism/break in (1)<br>• Individual needs to be present to cause damage (1) | 4 | Max 1 each if no example given. |

| Question | | | Answer | Marks | Guidance |
|---|---|---|---|---|---|
| **1** | **(c)** | **(i)** | Two from, two marks each e.g.<br>Hacktivist<br>• Hacks for social/politically motivated reasons (1)<br>• Involves releasing information/defacing websites (1)<br>• Disruptive rather than destructive (1)<br>Cyber terrorist<br>• Uses computers to cause fear/disruption (1)<br>• May have ideological/religious reasons (1)<br>• Not linked to a country/ anywhere in the world (1) | 4 | |
| **1** | **(c)** | **(ii)** | Two from, one mark each e.g.<br>• Limited programming knowledge/inexperienced / uses someone else's code (1)<br>• Most likely anti-social (1)<br>• Young in age (1) | 2 | |
| **1** | **(c)** | **(iii)** | Two from, two marks each e.g.<br>• Emotion/revenge (1) they might be bored/frustrated with a situation at work (1)<br>• Financial (1) paid by a competitor for information (1)<br>• Political (1) against the work being done for the government (1)<br>• Unintentional because of lack of knowledge (1) leaving printed data on a train (1)<br>• Convenience (1) circumventing policies to make their job easier (1)<br>• Personal use (1) sales person leaves company A and take customer list to company B (1) | 4 | |

| Question | | | Answer | Marks | Guidance |
|---|---|---|---|---|---|
| 2* | | | Indicative content may include:<br>• National security can be compromised leading to investigations by police which can disrupt research<br>• May not know what data the hacker has obtained or why they wanted it, can compromise their research and competitive edge.<br>• May remove money from bank accounts meaning bills with suppliers cannot be paid and new supplies cannot be ordered so work has to stop.<br>• Door systems could be compromised meaning that employees cannot enter the building or rooms within the building reducing their productivity.<br>• The email / communication system could be taken off line meaning that employees cannot send emails or access old emails limited the work they can do<br>• Files that are needed for the day to day work could be encrypted and not able to be accessed so further research cannot be done.<br>This is the day to day running of the company. | 7 | Level of response marking: |

| | | |
|---|---|---|
| L3 | 5 - 7 marks | Candidate has discussed the operational impact of a cyber security incident on Stevenson Research. The candidate is able to make informed and appropriate judgements within the context provided on the likely level of disruption and impact caused. An implied conclusion is present which is informed by the supporting analysis.<br>Subject specific terminology and knowledge will be clearly used to support and inform the assessment. |
| L2 | 3 – 4 marks | Candidate has described the operational impact of a cyber security incident on Stevenson Research. Impacts on the operation have been described and the candidate is able to make some judgements within the context provided.<br>Some subject specific terminology and knowledge will be used. |
| L1 | 1 – 2 marks | Candidate has identified the operational impact of a cyber security incident on Stevenson Research.<br>At the bottom of the mark band the candidate may have simply provided a single point about the impact of an incident on Stevenson Research |
| | 0 marks | Nothing worthy of credit. |

<table>
<tr><th colspan="3">Question</th><th>Answer</th><th>Marks</th><th>Guidance</th></tr>
<tr><td>3</td><td>(a)*</td><td></td><td>Indicative content may include:<br>• Testing will reproduce how a hacker may approach accessing the organisation and allow them to find the vulnerabilities and patch them.<br>• Testing will involve research into how the network has been set up allowing for decisions made in the installation to be confirmed.<br>• If testing does not find any vulnerabilities it still mitigates risk as it removes an element of possible attack.</td><td>10</td><td>Level of response marking:
<table>
<tr><td>L3</td><td>7 - 10 marks</td><td>Candidate has justified the use of testing for potential vulnerabilities as a way of mitigating risk. Positive benefits have been explained and the candidate is able to make informed and appropriate judgements within the context provided.<br>Subject specific terminology and knowledge will be clearly used to support and inform the explanations/evaluations.</td></tr>
<tr><td>L2</td><td>4 – 6 marks</td><td>Candidate has described how use of testing for potential vulnerabilities as a way of mitigating risk. Positive benefits have been described and the candidate is able to make some judgements within the context provided.<br>Some subject specific terminology and knowledge will be used.</td></tr>
<tr><td>L1</td><td>1 – 3 marks</td><td>Candidate has identified benefits of testing for potential vulnerabilities as a way of mitigating risk<br>At the bottom of the mark band the candidate may have simply provided a single point.</td></tr>
<tr><td></td><td>0 marks</td><td>Nothing worthy of credit.</td></tr>
</table></td></tr>
<tr><td></td><td>(b)</td><td></td><td>Two from, two marks each e.g.<br>• IDS is a monitoring system (detects) (1) whilst IPS is a control system (prevent) (1)<br>• IDS does not alter the packets (1) whilst IPS will prevent delivery (1)<br>• IDS requires a human to look at the results to take action (1) whilst and IPS will use an external database to take action (1)</td><td>4</td><td></td></tr>
</table>

| Question | | | Answer | Marks | Guidance |
|---|---|---|---|---|---|
| 4 | | | One mark each:<br>(i) Unauthorised (1)<br>(ii) Destruction (1)<br>(iii) Data/Information (1) | 3 | CAO |
| 5 | (a) | | Two from, e.g.<br>• Pretending to be a hacker (1) but it is authorised (1)<br>• A person/software that finds vulnerabilities (1) that can be exploited (1)<br>• Can be manual or automated (1) | 2 | |
| | (b) | | Two from, one mark each e.g.<br>• Fuzzing (1)<br>• Security functionality (1)<br>• Sandboxing (1)<br>• Testing patches (1)<br>• Social engineering (1) | 2 | Not penetration testing |
| 6 | (a) | | One mark for each line:<br><br>Incident Category: Minor; Critical; Negligible; Significant<br>Description: Little or no impact on the system or users; Can be handled internally IT support and security staff; Involves a serious breach of network security; Impact a small number of users and likely to disrupt non essential services | 4 | Allow use of numbers to link together.<br>Two or more lines from one box – no marks for that box.<br>Two or more lines to one box – no marks for that box. |

| Question | | | Answer | Marks | Guidance |
|---|---|---|---|---|---|
| | **(b)** | | Four from, e.g.<br>• So no stage is missed out (1)<br>• To gather all the information (1)<br>• Required to write the report (1)<br>• Not knowing who is on site when the attack occurs (1) might be someone not familiar with procedures(1)<br>• They will know what steps to take (1) and prevent errors being made (1)<br>• Can act with speed (1) to prevent further escalation (1)<br>• To identify who to contact (1)<br>• In management (1) | 4 | This is about procedures not the content |
| | **(c)** | | Two from two marks each, e.g.<br>• By knowing how they got in (1) the method can be closed (1)<br>• To stop someone else using the same technique (1) and accessing the network (1)<br>• To understand how the incident occurred (1) and if changes to policies are required (1)<br>• For legal reasons (1) to be able to report it to the ICO (1)<br>• To learn from the attack (1) and be prepared to counter it next time (1)<br>• To inform the police (1) so they can see if techniques has been used against other companies (1) | 4 | |

**OCR (Oxford Cambridge and RSA Examinations)**
**The Triangle Building**
**Shaftesbury Road**
**Cambridge**
**CB2 8EA**

**OCR Customer Contact Centre**

**Education and Learning**
Telephone: 01223 553998
Facsimile: 01223 552627
Email: general.qualifications@ocr.org.uk

**www.ocr.org.uk**

For staff training purposes and as part of our quality assurance programme your call may be recorded or monitored

**Oxford Cambridge and RSA Examinations**
**is a Company Limited by Guarantee**
**Registered in England**
**Registered Office; The Triangle Building, Shaftesbury Road, Cambridge, CB2 8EA**
**Registered Company Number: 3484466**
**OCR is an exempt Charity**

**OCR (Oxford Cambridge and RSA Examinations)**
**Head office**
**Telephone: 01223 552552**
**Facsimile: 01223 552553**

**© OCR 2021**

Cambridge Assessment

UKAS MANAGEMENT SYSTEMS 001