OCR
Oxford Cambridge and RSA

Cambridge Technicals Level 3

Information Technology

05838-05842 & 05877

Unit 3 Cyber Security

OCR Report to Centres June 2018

About this Examiner Report to Centres

This report on the 2018 Summer assessments aims to highlight:

- areas where students were more successful
- main areas where students may need additional support and some reflection
- points of advice for future examinations

It is intended to be constructive and informative and to promote better understanding of the specification content, of the operation of the scheme of assessment and of the application of assessment criteria.

Reports should be read in conjunction with the published question papers and mark schemes for the examination.

The report also includes links and brief information on:

- A reminder of our **post-results services** including **reviews of results**
- Link to **grade boundaries**
- **Further support that you can expect from OCR**, such as our CPD programme

Reviews of results

If any of your students' results are not as expected you may wish to consider one of our Reviews of results services. For full information about the options available visit the OCR website. If University places are at stake you may wish to consider priority service 2 reviews of marking which have an earlier deadline to ensure your reviews are processed in time for university applications: http://www.ocr.org.uk/administration/stage-5-post-results-services/enquiries-about-results/service-2-priority-service-2-2a-2b/

Grade boundaries

Grade boundaries for this, and all other assessments, can be found on the OCR website.

Further support from OCR

CPD Hub
Your route to OCR's teacher training

Attend one of our popular CPD courses to hear exam feedback directly from a senior assessors or drop in to an online Q&A session.

https://www.cpdhub.ocr.org.uk

CONTENTS

Cambridge Technicals
Level 3 Information Technology
(05838-05842 & 05877)

OCR REPORT TO CENTRES

Unit 3 Cyber Security

1. General Comments:

The continued improvement session on session was fully evident in this paper. Many candidates were able to cope well with the rigors of the paper and gave some really good answers.

However, there also remains a significant number of candidates who appear to be lacking any depth of understanding and knowledge. Whilst the unseen section of the paper is always going to be more challenging, section A can be prepared for and it was disappointing that many candidates seemed ill-prepared for this section of the paper.

2. Comments on Individual Questions:

Section A was based on the case study and associated tasks

Question 1 (a)

The vast majority of candidates were able to explain at least one reason why personal information should be protected, with most being able to explain two reasons. In a few cases, candidates knew why personal information should be protected, but gave weak expansions, such as “because he does not want someone else to know things about him”. Answers such as this, which are extremely general, as not sufficient for this level of examination.

Question 1 (b)

There are many items of information that may be garnered by accessing a digital personal assistant. As a consequence, the vast majority of candidates gave two good answers for this question. In a very small number of instances, candidates did not seem to fully appreciate what a digital personal assistant is and so gave answers that were not acceptable within the breadth of answers accepted.

Question 1 (c)

Whilst the breadth of possible answers for this question did not match the breadth of the previous, examiners were aware that many possible answers existed and awarded accordingly. However, answers such as “his address” were not accepted.

Question 1 (d)

This question required candidates to describe two types of cyberattack that could be carried out and which would obtain personal data from Mr Daka. This description had to be of the method employed, so the first mark for each description was awarded for the identification of the method. The second mark was the expansion to give a description.

Many candidates gave good answers here, with Phishing, Pharming and Social Engineering all appearing regularly. However, candidates who simply stated “hacking” were not awarded a mark, and neither were candidates who suggested methods, such as physical assault.

Question 1 (e)

The vast majority of candidates realised that the digital personal assistant had direct control and access to physical controls, such as doors and heating and therefore any third party control was a potential risk. Answers tended to concentrate on the physical risk caused by opening doors/disabling locks and these answers were generally well explained. However, the second answer, usually focussing on access to heating, was not well explained, with candidates simply stating that heating could be turned up.

Question 2

This question focussed on the types of attackers who could target a digital personal assistant and their motivations.

Question 2 (a)

For question 2 (a), the key point about a vulnerability broker was that they sell, or attempt to sell, data. Where candidates simply stated that a vulnerability broker stole information, or looked for easy access to systems, this was not sufficient, as these definitions were not considered specific enough.

Question 2 (b)

This question proved to be quite a challenge to many candidates. One acceptable answer was that the broker would have data about Mr Daka, but all others were to do with any concern Mr Daka should have in general terms.

Most candidates appreciated that the broker could sell information to a third party, with a negative outcome, but were then unable to give any further impacts. This would suggest that many candidates had prepared by considering impact on Mr Daka, but had not prepared by considering wider impacts.

Question 2 (c)

A significant minority of candidates missed the advice that they should give motivations other than financial. Where candidates gave answers that could lead to financial gain, but could equally lead to non-financial gain (such as identity theft) and did not specifically state that the outcome would be a financial gain, marks were awarded.

Where candidates did take note of the direction, many marks were awarded. This area of the syllabus would appear to be a strength, with many candidates scoring very well indeed.

Question 2 (d)

As with question 2 (b), candidates failed to take note of the context of this question and gave general answers about individual attacks on individual digital personal assistants. However, the

question was actually about an attack on the brand of the digital personal assistant and therefore was looking for an understanding of the interaction between a digital threat and business. Very few candidates scored any marks for this question.

Question 3 explored candidates' understanding of wider areas of vulnerability.

Question 3 (a) and (b)

As a cohort, candidates did not seem confident with either of these areas. In a few cases, candidates showed good technical understanding of network vulnerabilities and earned good marks. However, the majority of candidates gave general answers that showed little technical understanding. Similarly, with question 3 (b), candidates knew that fuzzing was an attack, but few knew the fundamental point that this form of attack overloads the system with data.

Section B assessed knowledge from across the syllabus and is not linked to the scenario.

Question 4

This question focussed on methods of security management.

Question 4 (a)

Many candidates scored well here, with most candidates focussing on the area being monitored.

Question 4 (b)

This question assessed understanding, as well as candidates' ability to express themselves eloquently.

Candidates were asked to evaluate the use of an IDS system to protect a network. Where this was answered well, candidates gave full answers that discussed the positive aspects of an IDS as well as the negative aspects. These answers were balanced, well expressed and evaluative of the overall impact.

However, other candidates made a few simple points about IDS and did evaluate their usefulness, whilst others made a few points and went onto discuss other methods of protection. Whilst a discussion of other methods of protection may be seen as a supporting point to a general discussion of IDS, this is most definitely not a sound answer when used on its own.

Question 5 (a)

As with other questions in this paper, the main question directly excluded possible answers that candidates may give. Despite this, many candidates gave answers that were simply based on the method used and so could not be considered.

Where candidates did give other answers, many correctly identified that time spent in the system was a key indicator of the skill of the attackers, as well as the areas of the network to which the attacker was able to gain access. However, other candidates wrongly considered that the

nature of the data stolen, or the impact of its theft, were important. Neither answer was acceptable.

Question 5 (b)

This was well answered by many candidates, who were fully aware that a great deal could be learnt by investigating the techniques used by attackers, and that this information could be used by the investigators themselves and others.

About OCR

OCR (Oxford Cambridge and RSA) is a leading UK awarding body. We provide qualifications which engage people of all ages and abilities at school, college, in work or through part-time learning programmes.

As a not-for-profit organisation, OCR's core purpose is to develop and deliver general and vocational qualifications which equip learners with the knowledge and skills they need for their future, helping them achieve their full potential.

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

OCR Customer Contact Centre

Telephone: 02476 851509
Facsimile: 02476 421944
Email: vocational.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