BTEC

L3 Lead Examiner Report 1901

January 2019

L3 Qualification in Information Technology

Unit 11: Cyber security and incident management

Pearson

Edexcel and BTEC Qualifications

Edexcel and BTEC qualifications come from Pearson, the world's leading learning company. We provide a wide range of qualifications including academic, vocational, occupational and specific programmes for employers. For further information visit our qualifications website at http://qualifications.pearson.com/en/home.html for our BTEC qualifications.

Alternatively, you can get in touch with us using the details on our contact us page at http://qualifications.pearson.com/en/contact-us.html

If you have any subject specific questions about this specification that require the help of a subject specialist, you can speak directly to the subject team at Pearson. Their contact details can be found on this link:
http://qualifications.pearson.com/en/support/support-for-you/teachers.html

You can also use our online Ask the Expert service at https://www.edexcelonline.com
You will need an Edexcel Online username and password to access this service.

Pearson: helping people progress, everywhere

Our aim is to help everyone progress in their lives through education. We believe in every kind of learning, for all kinds of people, wherever they are in the world. We've been involved in education for over 150 years, and by working across 70 countries, in 100 languages, we have built an international reputation for our commitment to high standards and raising achievement through innovation in education. Find out more about how we can help you and your learners at: www.pearson.com/uk

January 2019
Publications Code 20158K_1901_ER

Grade Boundaries

What is a grade boundary?

A grade boundary is where we set the level of achievement required to obtain a certain grade for the externally assessed unit. We set grade boundaries for each grade, at Distinction, Merit and Pass.

Setting grade boundaries

When we set grade boundaries, we look at the performance of every learner who took the external assessment. When we can see the full picture of performance, our experts are then able to decide where best to place the grade boundaries – this means that they decide what the lowest possible mark is for a particular grade.

When our experts set the grade boundaries, they make sure that learners receive grades which reflect their ability. Awarding grade boundaries is conducted to ensure learners achieve the grade they deserve to achieve, irrespective of variation in the external assessment.

Variations in external assessments

Each external assessment we set asks different questions and may assess different parts of the unit content outlined in the specification. It would be unfair to learners if we set the same grade boundaries for each assessment, because then it would not take accessibility into account.

Grade boundaries for this, and all other papers, are on the website via this link:

http://qualifications.pearson.com/en/support/support-topics/results-certification/grade-boundaries.html

Unit 11: Cyber security and incident management

Grade	Unclassified	Level 3			
		N	P	M	D
Boundary Mark	0	12	24	40	57

Introduction

Although the overall specification was first examined in 2017, this was the first January sitting for Unit 11, Cyber security and incident management and the majority of centres were new.

The examination is based on a scenario and consists of five activities, three in Task A and two in Task B.

Task A involves the production of a risk assessment and cyber security plan for a specified network. Task B involves the analysis of a reported cyber security incident relevant to the specified network.

Introduction to the Overall Performance of the Unit

It was clear from the scripts seen that most of the learners were able to understand the scenario and produce the required documents. A significant number however seemed to rely on generic responses which were clearly derived from the SAMs and the 1806 paper. e.g. WiFi issues, which were not mentioned in the 1901 scenario and use of NFC cards which were a feature of the 1806 paper.

The ability of learners to perform the two tasks, was surprisingly different, with some giving good answers to one task but seemingly floundering in the other. Although the activities require somewhat different skills, it was expected that learners would perform evenly over the whole examination.

Individual Questions

Task A

Activity 1 – Risk assessment of the networked system

This activity requires learners to assess the cyber security implications of the scenario and produce a risk assessment. A risk assessment template is provided, together with a simple matrix for determining risk severity.

Nearly all the learners managed to fill in the template with estimates of threat probability and size of loss, but a disappointingly large number were then unable to use these estimates to look up the correct severity value in the matrix.

The first example shows a poor usage of the template, with an ill-defined threat and vague wording for the explanation.

Threat number.	10
Threat title.	Virus
Probability.	likely
Potential size of loss / impact level.	Major
Risk severity.	High
Explanation of the threat in context.	The threat of a virus is high because certain workers or visitors could go on to a site they are not suppose to be and on and they could download the virus of the website they where on and how it has now been transport to the company's computer and now the company's computer will now have malware on it and it won't work as well as it should do.

The next learner gives a good estimate of the risk but does not clearly identify the threat, although in this case the explanation makes up for the weakness of the threat title. It would be better to title it something such as 'weak passwords for admin level access to the server'. This learner has also put some of the explanation of the threat in the 'Potential size of loss' box.

An inability to complete the template correctly is likely to impinge on the Technical Language mark and may also lead to poor planning for subsequent activities.

Threat number.	4
Threat title.	Breach due to weak password.
Probability.	Unlikely
Potential size of loss / impact level.	Possible breach to the CE server due to weak password security.
Risk severity.	High
Explanation of the threat in context.	As peter has given more people administrative access there is a bigger risk of targeted attacks and if there is a weak password to gain access to the server and somebody finds it out there could be a possible security breach and an attacker can gain access to the server and possibly shutting it down.

The final example shows correct usage of the template and is worthy of band 3.

Threat number.	8
Threat title.	Employees or the dedicated players acting as 'guides' and 'trouble-shooters' could sabotage the game, network or the servers for their own reasons.
Probability.	Unlikely
Potential size of loss / impact level.	Major
Risk severity.	Medium
Explanation of the threat in context.	This threat can be caused due to employees not being happy about certain things that are taking place in the business or about the development and management of the game. This risk is not likely to happen but if it were, the consequences for it would be very significant and major. The potential size of loss is major because the dedicated players would be given enhanced access to the game servers at Romwebhost and if they were going to sabotage the servers and the network, then they could potentially cause a lot of damage.

Other common errors were:

- the identification of non-cyber security threats such as burglary or fire. These threats are not penalised in the marking but learners who identified several such threats tended to get lower marks because they (a) spent valuable time on them and (b) usually only identified a small number of actual cyber security threats as they had already filled a page or two with the non-cyber threats.
- repeating the same cyber security threat, e.g. viruses in the server, the

network, the PCs, etc. each being specified as a separate threat.

Activity 2 – Cyber security plan for the networked system

This activity requires learners to produce a cyber security plan based on their risk assessment from Activity 1. A template is provided for learners to complete.

As with Activity 1, the great majority of learners used the template correctly. Those who could not or would not do so were likely to gain lower Technical Language marks.

Although the threats dealt with in Activity 2 should be the same ones that are risk assessed in Activity 1, marking of Activity 2 is independent of Activity 1. This means that an erroneous estimate of threat severity or overemphasis on generic risks does not directly affect the marking. Although having a number of non-cyber security threats is disadvantageous for the reasons given for Activity 1.

Activity 2 requires that the learner demonstrate an understanding of the threats that they have identified. They also must tailor protection measures and testing to meet those threats.

Top band answers do not need to be perfect but a good answer such as the one below uses all the headings in the template and gives sufficient detail to demonstrate understanding of the threat and how it can be countered.

Where one of the constraints has little or no relevance, learners should say so rather than leave the heading out. This indicates that the learner has considered the matter and not simply ignored it.

" **Protection Measure 1 – Anti-Virus Software:**
Threats addressed – Malware
Details of action to be taken – Anti-Virus software is to be installed on all systems to ensure that any form of malware uploaded to the network is unable to infect either the servers or the workstations, keeping player accounts, worlds and the game itself free from attack.
Reasons for the actions – this preventative measure will actively protect the network from all known forms of malware, as well as identifying files or programs that may act in malicious ways and reduce the threat of

theft or destruction.
Overview of constraints – In some cases, effective AVS can be expensive and so care must be taken to choose a program that will keep the network free from attack, but will not cost so much as to bankrupt the developer or Romwebhost.
Overview of legal responsibilities – Romwebhost must ensure that they have paid for the AVS and have the correct licences that prove they are allowed to use it in a commercial capacity.
Overview of usability – The usability of the system should not be affected by this addition, though it may be that some tasks are flagged as malicious where they were not before and so steps must be taken to allow them through the software.
Cost-Benefit – The benefits of this protective measure definitely outweigh the costs, as it will prevent the infection of systems on the Romwebhost network and prevent the loss of game data, and in turn the loss of players and revenue."

The test plan should of course match the identified threat. It does not need to be particularly detailed as the system is hypothetical and learners cannot be expected to know the exact set up. It should however consist of relevant tests that could reasonably be carried out as shown in this example.

Test No	Test description	Expected outcome	Possible further action following test
1	Attempt to run a benign, but malicious-looking file or program	The AVS should flag it as malicious and prevent the user from accessing it	
2	Attempt to run a form of malware that the AVS knows	The AVS should prevent the malware from executing and quarantine it	If it is preferred that the malware should be destroyed instead of quarantined, this can be done in the settings.
3	Attempt to run a program necessary for work	The AVS should not prevent it from running	If the AVS flags it, it should be allowed to run through the settings.

The next example although addressing reasonable situations, a botnet attack and access rights, does not have any tests. The test description and expected outcome give a reasonable idea of what the tests would be for, but do not have enough information about what the tests would be. The possible further actions are really actions that should have been taken before testing to see if they were effective.

Test No	Test description	Expected outcome	Possible further action following test
1	Security and connection of the servers	Secure connection that wouldn't allow easy botnet attack	2 way access into the server as they will allow for a much stable and secure connection. The botnets would be less efficient as there will be another security path on the way. The cost of eliminating botnets is low however it is a huge benefit for the company as there will be less stress on the server.
2	Permission check	Guides don't have any access that would allow them to access the admin console	Hire trusted people into the company as administrators in order to take care of the players and servers. The cost might be depending on the amount of work and responsibilities. This would be a huge plus for the game as there would be someone to help players with difficult situations in the game as usually when a new game starts there is a huge amount of bugs (errors within the game) that have to be fixed.

Activity 3 – Management report justifying the solution

The result of this activity should be a Management Report, justifying the solution presented in the previous activities.

Learners are told that:

The report should include:

- *an assessment of the appropriateness of your protection measures*
- *a consideration of alternative protection measures that could be used*
- *a rationale for choosing your protection measures over the alternatives.*

Learners should also be able to analyse the information from the scenario to determine at what level to pitch the report. They were told:

Peter Russof is a computer programmer specialising in developing games for PCs. He has written several stand-alone games and has built up a profitable business as an independent game producer.

Elana runs a web hosting company in Romania, Romwebhost.

This, together with other information in the scenario indicates that Peter and Elana are likely to understand technical terms but are probably not experts on cyber security and that the language should be accessible to a non-specialist.

It is expected that a top band report would be laid out correctly, including; a title, a summary or introduction, a main body split into sub-titled sections or bullets, and a section with conclusions or recommendations. Although this final section could be integrated into each of the ones in the main body.

The Technical Language trait is assessed over the whole of Task A, but the ability of a learner to use an appropriate report format and to pitch the language at a suitable level for the target audience will certainly influence the mark awarded.

Task B

Activity 4 – Forensic incident analysis

In this activity learners must analyse both the Task B scenario and the evidence items that are presented. The scenario will be related to the one from Task A but will be shifted in time, location, or both. In this case the Task B scenario occurs a few weeks later than the Task A scenario, when Peter has migrated his game to the Romwebhost servers in Romania.

The learners are given a template to copy and complete for each piece of evidence that they consider. Most candidates managed this successfully, although many did not do anything about the evidence contained in the Client Brief and Set Task Brief. An inability to complete the template correctly is likely to impinge on the Technical Language mark for Task B.

Learners were told that they did not need to look at evidence item 5, the policy document, for this activity. Many did however and this would have penalised them by wasting time.

Many learners produced weak answers for reliability of the evidence, even fthose with higher band marks. The work on the email and the meeting notes was particularly poor. Too many learners thought that the redactions in the email were on the original and so stated that the origin was dubious and the email could not be relied on. None of the learners realised that the notes from the meeting would be classified as minutes and therefore a legal document which must be accurate.

The template calls for a conclusion to be drawn from each individual piece of evidence as well as an overall conclusion. Learners need to understand that individual pieces of evidence may not lend themselves to any particular conclusion and any one piece of evidence taken by itself is unlikely to give the full picture. Learners who omitted the overall conclusion tended to be restricted to lower band marks.

Most learners realised that the incident hinged on the passwords. Unfortunately, many then went on to say that they must have been stolen from the database, despite the fact that evidence item 4 states that no passwords are kept, just the hashes.

"They were able to resolve the problem and prevent further

attacks. This was done by the reset of password to all users other than those who had already reset their passwords. This resolution has led me to believe that the attacks were done by accessing the database once, this is due to the reset of passwords being the resolution. If the attackers had access to the database, they would still be able to steal data such as passwords and proceed with further attacks. This could have been done through multiple methods such as, creating a copy of the database via internally connecting to the servers, phishing an employee into giving them a copy of the database or releasing the account information."

Another common answer was a phishing attack.

"I think it is possible that the hacker has conducted a phishing attack by using the players' username to figure out their email addresses then find out their passwords. If this happened, then it is highly possible that they have done this through the use of spear phishing emails that were somehow infected with key-loggers possible, which then helped the hacker to gain access to the players' accounts".

This is certainly possible but there is nothing in the evidence items to point directly at that solution and a blanket password change for gamers would not have stopped further phishing attempts.

The more probable answer is that the passwords were already 'in the wild' due to previous database breaches at other companies.

"My overall conclusion is that the incident is not actually the fault of Romwebhost and is more like a data breach of another company that has been utilised by hackers to test the stolen data to see if they can use it to get into accounts of CE players. There seems to be a lot of supporting evidence to this such as accounts not having any more problems after changing passwords, them not being able to find evidence of a breach of any kind and the fact that they could get users names from previously exposed emails and then match stolen passwords."

Activity 5– Management report on security improvements

The result of this activity should be a Management Report. As with Activity 3, the report should look like a report and be written at a level suitable for the target audience.

It is expected that a top band report would be laid out correctly, including; a title, a summary or introduction, a main body split into sub-titled sections or bullets, and a section justifying the conclusions or recommendations. Although this final section could be integrated into each of the ones in the main body.

Learners are told that:

Areas for improvement are:

- *adherence to forensic procedures*
- *the forensic procedure and current security protection measures*
- *the security documentation.*

Although Activity 5 is marked independently of Activity 4, there is inevitably a close link between them, since learners who were unable to reach at least plausible conclusions in activity 4 would be hard pressed to identify and combat the weaknesses inherent in the scenario.

Good answers concentrated on the mistakes made.

"Firstly, the use of personal information to create a username was a mistake. Personal information such as that should not have been allowed to be displayed publicly within the game and all players should have been prompted to create their own, unique username upon account creation. Secondly, accounts should have been protected from attacks like this using two-factor authentication to ensure that only the account's creator could access it using a code generated and displayed on their personal mobile device. "

"In regards to forensic procedures, Romwebhost's cyber security manager acted well in enforcing a password change for all players as this immediately prevented the attacker from accessing and vandalising more accounts, however efforts should have been made to determine if each account was being accessed from the same geographical location or IP address each time so that the perpetrator could be more easily identified, or their IP blacklisted from connecting to the main CE server at all. Also, during the actions taken by the first-line technician to restore player accounts the password change should have been enforced straight away to ensure the account was not again compromised during the restoration."

"Peter was right to take into account past security breaches of other game developers and learn from their mistakes in order to build a more secure login system, guarded against similar attacks. However, it was wrong of him to focus only on password security and instead he should have looked at the security and privacy of players' personal information as a whole. Also, upon the third failed login attempt an email notification should be sent to the account holder to ensure they are made aware of the attempts to access their account so that they could take action and change their username or password if they feel it necessary to ensure security of their account."

"When Alex checked the SQL filters and server security, he should have made detailed notes on what he found. Even if these were completely unaffected in the breach that is still important evidence in confirming that the breach was not the fault of Romwebhost or CE, which would have proved useful if the case had in fact gone to court."

Less good answers had a mixture of mistakes, statements about the system, and possible solutions.

"During this incident I believe the CE and romwebhost security were efficient at reporting and documenting the incident, and did a job at assisting the effected users after the incident had taken place. Although the security team did a good job of securing the situation, I believe some improvements could be made in the future to deal with this sort of incident quicker, or prevent it in its entirety. The first improvement would have been to take action on the threat, instead of observing while peoples accounts were hacked. These accounts could contain a user's personal information, as well as any residual payment methods that they could have used on the forum. This seems to be a mistake on the cyber security's part. The security team already understood the situation, so there was really no need to allow the account breaches to escalate for a few more days

before warning players and forcing a password change for every user. I believe that many account violations could have prevented if the security team would have taken action in a quicker manner."

In the security documentation section, good answers both identify the weakness and give a suggested replacement or additional text to be used.

"On first glance the security documentation seemed to be good however then I realised one glaring problem there is no response procedure for the theft of personal information/data, for the breach they seemed to have followed the section 'Theft of company data' whilst this still gets the job done and has some very similar points in it there needs to be a different section modelled towards handling situations involving personal information/data. It could be modelled as follows:

(c) Theft of personal information/data

- *o Theft or loss of personal information may occur in a number of ways.*
- *o Any loss of personal information/data should be reported at once to CSIRT team leader, initially a verbal report must be followed up by an email. Both the Cyber Security Manager and Elana should be consulted about this as it is a very serious situation.*
- *o The CSIRT must then investigate the loss and identify exactly what was stolen, how it was stolen and if possible who by. They must also check to see if the customer complaining is actually an account holder.*
- *o Having identified the items above Elana must then inform the police, so a formal investigation can be launched and the culprit found, and customers, so they know if anything such as unauthorised bank transactions go through why that has happened.*
- *o If there was damage to the accounts, they then need to restore them using a backup.*
- *o The security should then be overlooked and the security team should implement procedures to prevent future losses."*

Summary

Based on their performance on this paper, learners should:

- learn how to use the templates before the examination date. The templates are fixed and will be used for every examination
- learn how to set out a formal report, the suggested sub-sections are fixed and will be asked for in every examination
- read the scenario carefully, looking for specific mentions of security threats, and worries or concerns of the people involved
- avoid the pre-planning of answers based on the sample assessment material or previous examinations. Although many of the threats will be similar, the context will be different
- ensure that the risk severity is plausible
- look at all the evidence. This includes the scenario as well as the individual evidence items
- look at each evidence item separately to draw a conclusion for that evidence item
- look at all of the evidence holistically to come to an overall conclusion. This may contradict an individual conclusion
- refer to specific sub-sections / pieces of text when discussing changes to the Incident Management Policy