Examiners' Report
Lead Examiner Feedback

January 2021

Pearson BTEC Nationals
In Information Technology (20158K)
Unit 11: Cyber Security and Incident Management

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 2021
Publications Code 20158K _2101_ER

Introduction

The examination is based on a scenario and consists of five Activities, three in Task A and two in Task B.
The tasks and mark schemes are fixed but the scenario changes for each examination.
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

Although there were a limited number of scripts due to COVID 19, the majority of those seen showed that learners were able to understand the scenario and produce the required documents.

As in previous series, too many had learned generic responses. These learners seemed to be unable to adapt these responses and included generic threats and measures which had little or no relevance to the scenario. This does not prevent learners from passing the examination but restricts them to band 2 marks due to them not meeting the criteria for anything higher.

The ability of learners to perform the two tasks was often 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 matrix weakness has been noted in previous reports and shows poor preparation by the Learners and their centres.

In this examination series a significant number of learners failed to differentiate between the 'existing' system and the 'proposed' system that they were asked to risk assess. A lot of time was therefore wasted writing about the 'existing' system. Marks are not subtracted for this, but the learners are self-penalising by using up time.

The first example shows a poor usage of the template. The threat is plausible although the explanation is muddled. The size of loss is hedged but can be taken as 'high'. This value is not in the matrix, neither is the probability of medium, so the risk severity, high, cannot be obtained from the risk matrix.

Threat number.	2. Development plan
Risk severity.	High
Threat title.	Internet access via router
Probability.	Medium
Potential size of loss / impact level.	The potential size of loss could be high if in the router system log on unathorised person.
Explanation of the threat in context.	The router in the estate office should only be used by the CME staff which includes the technical manager, joanne Reedsman and two electricians. When login to the computers in the office the person should be authorised in the system, so it can use the the computer office. The person using specifeid pc sohuld used secure password

The second example shows correct use of the matrix and is a Band 3 response.

Threat number.	002.)
Risk severity.	High
Threat title.	Social Engineering Techniques To Gain Administrative Privileges
Probability.	Likely – as it states that the electricians and the Technical Manager can deal with the minor IT problems, but call in the outside contractors whenever it is necessary implying that they are inexperienced.
Potential size of loss / impact level.	Major - as using Social Engineering techniques is a major threat to any organization, business or estate and can cause internal and external damage.
Explanation of the threat in context.	Social Engineering techniques to gain administrative privileges is a dangerous and impactful threat that can occur to the Estate. This threat could happen through the use of cyber-attackers using Social Engineering techniques i.e. Phishing to gain access to administrative privileges to cause potential damage to the Estate and use it for their own benefit. They commit to doing this as it says in the scenario that he uses CME' administrative staff for most of the computing task, this indicates that the owner (Andrew Caelcabben) is experienced in his management, which is estate management, but he is not a specialist in his job, and the threat of allowing administrative staff for most of the computing tasks, means that you won't always know what they could do with most of the tasks. The disadvantage of this is that cyber-attackers could use Social Engineering techniques for example phishing to deceive and manipulate people into giving making specific users give them their personal details such as their name, telephone number or even their address. This can lead to a reputational loss as Caelcabben Manor Estate will lose a vast amount of customers due to this cyber-attack as they will lose the trust of the Estate. Additionally, this can eventually lead to a financial loss as due to this huge and impactful cyber-attack, the Estate will lose a massive amount of revenue which can lead to unexpected events such as bankruptcy for the Estate if the financial loss is that bad.

Some common errors were:

- the identification of non-cyber security threats such as multiple ways of damaging equipment. One instance of this would be appropriate but having break-ins to each building on the estate as separate threats is not helpful. 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 other security threats as they had already filled a page or two writing about physical ones.

- repeating the same cyber security threat, e.g. viruses, malware, trojan, worm, etc. each being specified as a separate threat.

- assuming that Linux, e.g. as specified for the servers, was less secure than Windows being used for the same purpose.

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.

Threat number: 4
Threat title: Accidental deletion of data
Actions: Store backups off site in a secure location
Reasons: If data is accidently deleted, it could also be accidently deleted from the backup as it is connected to the server. Therefore it is important to, when the disk is imaged, also image it onto a separate hard drive to make sure that there is always a secure copy of the data. This also adds another layer of protection against physical security threats, malware and data corruption, as this backup will be kept in a secure location, away from the threats, it will not be effected by them, allowing the company to successfully save/restore all their data in the event of one of the aforementioned threats
Constraints:
There are very little constraints, as imaging the data stored on the server onto another HDD requires very little technical knowledge and the hard drive itself will be inexpensive
Legal: The data that is imaged onto the separated hard drive will need to be kept secure and safe in accordance with the data protection act or CME will risk a fine

Usability: This action has little to no impact on the usability of the system, all that has changed is that, when disk images are taken, the same data is imaged onto another hard drive

Cost - benefit: The cost for this action is very low and the potential benefit in case of accidentally deletion of corruption of data is very high so I believe that his has a high cost benefit

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 the example.

Test plan

Test No	Test description	Expected outcome	Possible further action following test
1	Have the system backup a set of data and then go through it to ensure all required data has been backed up	All the data will be successfully backed up onto the network attached storage device.	If the data has not been successfully backed up then the backup system will need to be revised/fixed

The next example shows a reasonable measure, staff training, but does not link it to a threat.
The learner's answer, although filling the template correctly, does not give any insight into why they think training is appropriate in the context of the scenario.

Protection Measure 2: Staff Training

Details Of Actions To Be Taken: The details of the actions that need to be taken are that staff members that work for businesses or even organizations need to make sure they undergo staff training at least once in their jobs. There are different types of staff training that they will need to go and these can stem from i.e. project management and staff management so they will need to make sure they adhere and obide by these different sets of training that is instructed/given to them by their organization.

Reasons For The Actions: Staff members will need to be put under staff training in order to improve themselves and help themselves advance in their careers and to also help them improve and enhance the productivity of the organization that they work for.

Overview Of Constraints – Technical And Financial:

Technical Constraints: The technical constraints of this is that, there are downsides to staff training and that is why CME must make sure that each staff member must perform staff training effectively, otherwise they can fall in the trap of making a mistake, which could prove costly to that employee.

Financial Constraints: Staff training can be very expensive to organize for each staff member (per staff member), so some organizations, even they all have to undergo it, may feel a bit hesitant and might have second thoughts and would have to consider carefully before they instruct and perform staff training on their employees. Overview Of

Legal Responsibilities: CME will need to make sure that they have the correct legalisation and the correct license to perform staff training in their estate. If they don't, this could possibly result in a hefty fine or prosecution, so they must make sure they adhere to the legal rules before doing this.

Overview Of Usability Of The System: The overview of the usability of the system is that staff members must make sure that, whilst they are performing their staff training, they must have a certain goal or objective in mind to consider whilst doing this. They must make sure with each staff member and find out different techniques and methods to make sure that their goals and objectives can be achieved.

Outline cost-benefit: The benefits and advantages of using staff training for CME will greatly outweigh and exceed the costs of using staff training per each member.

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:

Andrew has many years of experience in estate management but considers himself an IT user rather than an IT specialist. He uses CME's administrative staff for most

computing tasks.

This, together with other information in the scenario indicates that Ben is unlikely to fully understand technical terms and may only have a limited knowledge of cyber security terms. The report should therefore 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.

The following extract shows a part of a good example of a management report. It addresses Andrew's requirement from the development plan.

Andrew wants a robust backup system. He is considering using RAID 1 on the two servers and a network attached storage device to store recovery files and periodic disk images.

Cloud backups

Appropriateness of protection measure

Andrew wants a robust backup system, the best way to do this is to use a cloud storage service and take consistent incremental and full backups. Over time the cost of the subscription to the cloud storage service will outweigh the cost of the planned NAS however it will be more secure and less susceptible to threats such as sabotage.

Alternative protection measures

An alternative is to use an onsite NAS with regular incremental and full backups, this will include a high initial cost and maintenance costs however in the long term will be cheaper than cloud storage. By being on site it will not be likely that they lose access to their backups unlike cloud storage where the provider could be attacked or internet access may not be available. The NAS will be susceptible to threats such as sabotage and malware such as worms which will significantly more damage if they destroy the data on the NAS.

Rationale for choosing the original protection measures

Cloud storage service providers rarely have issues and it is unlikely for internet access to be lost just as their main servers are attacked, by having on site storage the backup data is being put at unnecessary risk and could lead to massive financial, operational and reputational loss as they lose access to confidential data that legally needs to be protected securely.

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 at the same location but at a later time, after the changes discussed in Task A have been implemented.

The learners are given a template to copy and complete for each piece of evidence that they consider. Most candidates managed this successfully, although most 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. Some did however and this would have penalised them by wasting time.

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.

In evidence item 2, The email, the attacked makes some claims about what has happened.

When you were viewing, your browser started out operating as a Remote control Desktop that has a keylogger which provided me with access to your screen as well as webcam. Just after that, my software gathered your complete contacts from your
social networks, as well as Outlook addreses and then i made a double video.

Too many learners took this at face value, despite it being from the attacker and despite other evidence items making the claims very dubious.

Those learners who applied their analytical skills more thoroughly were able to explain why the attack could not have taken place as claimed. There is no absolute, correct answer but the next example gives a good summary of the evidence pointing to an untargetted attack.

The email Chelsi received was mostly false and was just used as empty threats. One of the retail websites she may have used could have easily been breached, explaining how the emailer had her password to the account, and possibly Andrews email and password as well, as they may have used the same site previously and the database may have still had both of their data stored at the time of attack. The report confirms that there are no existing threats at CME that could have lead me to believe that a key-logger was/is active on their systems due to the scans that CME ran on all of the devices, which came up negative for any potential threats. Unfortunately due to the lack of information on the devices Chelsi used, there is no possible way to confirm that she couldn't have webcam footage of her using a device, however if she didn't use a windows laptop at all, it's not possible for there to be any footage of her using the machines. To conclude I think that it is entirely more likely that an external source suffered a data breach rather than CME themselves, due to the lack of true evidence provided by the emailer that he had any video or data about Chelsi or Andrew other than their passwords. The email also would have been less likely to be sent if a key-logger was active, due to Chelsi inputting both her and CME Credit Card details, which could have been of more value to the emailer than an empty threat about a small amount of bitcoin. It is more likely that the email was just a spam phishing email that was mass sent to everybody registered for the retail sites that utilised buzzwords and scare tactics.

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 included:

- a section on the mistakes made. e.g.

To improve the security of the system CME employees must adhere to the security response plans detailed in evidence item 6. The incident response procedure for infection of CME systems with malware is to report the system immediately and to and shut down the system as soon as possible, neither Chelsi nor Andrew adhered to this policy. When Chelsi received the threatening email originally it was at 13.55 on the third, she did not report it until 9.15 of the 4th. This leaves a window of half a working day where Chelsi suspected that her system had been infected by a key logger/other malware and did not report it and presumably continued to use the computer through the rest of the day. If the system really was infected with malware (which I believe it wasn't) during this time the malware could have spread of other systems and placed the rest of the network in danger. Andrew committed a similar offence, when he received the malware he suspected a key logger and only reported the offence to the CSIRT once he had been asked about it.

- a section on the security documentation. e.g.

To improve the security response of CME/ the CSIRT, a wider range of security incidences must be covered on the response procedures (such as social engineering) so that the CSIRT can be ready to quickly respond and contain the threat should one occur, it also ensures that the other staff know what to do if the encounter one of the threats and know how to act accordingly. This could have prevented or minimised the risk caused by this breach if Chelsi had recognised the email as social engineering and reported it sooner to the CSIRT.

- a section on recommendations e.g.

Suggestions:

• Strong password policy
• Staff training with cyber-attack related issues
• Produce an internet usage policy on the workplace
• Access rights on the use of peripheral devices
• Adherence to forensic procedures
• Safe working practices
• Configure the email filtration

Strong password policy- as seen with the usage of a weak password by the employees which was easy to track. The organisation must train their employees to use a strong password for user authentication with passwords containing a combination of letters, numbers, special character, lowercase and uppercase alphabets, and a good character length up to 8 characters minimum. This will

ensure that the password is not easily compromised by hackers trying to gain unauthorised access to the network.

Less good answers had a mixture of mistakes, statements about the system, and possible solutions. There was often no clear structure to the report, with learners failing to use the supplied structure.

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.

Pearson Education Limited. Registered company number 872828
with its registered office at Edinburgh Gate, Harlow, Essex CM20 2JE