L3 Lead Examiner Report 1906

June 2019

Level 3 Nationals
Information Technology

Unit 11
Cyber security and incident management (20158K)

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

Publications Code 20158K_1906_ER

June 2019

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		
		P	M	D
Boundary Mark	0	24	40	57

Introduction

The overall specification was first examined in 2017, this was the second summer sitting for Unit 11, Cyber security and incident management. The first summer sitting had a small number of entries and many of the 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 the majority of 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 earlier papers.

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 fairly evenly over the whole examination.

Individual Questions

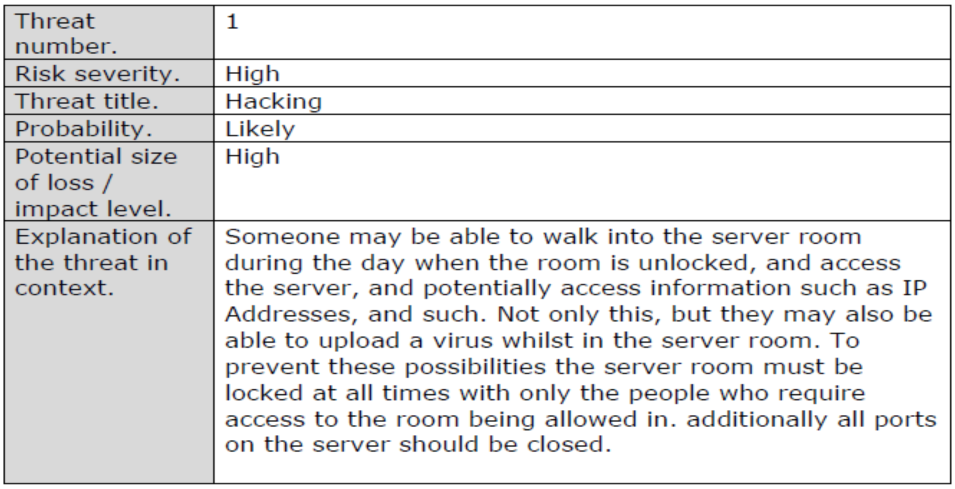
Task A

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.

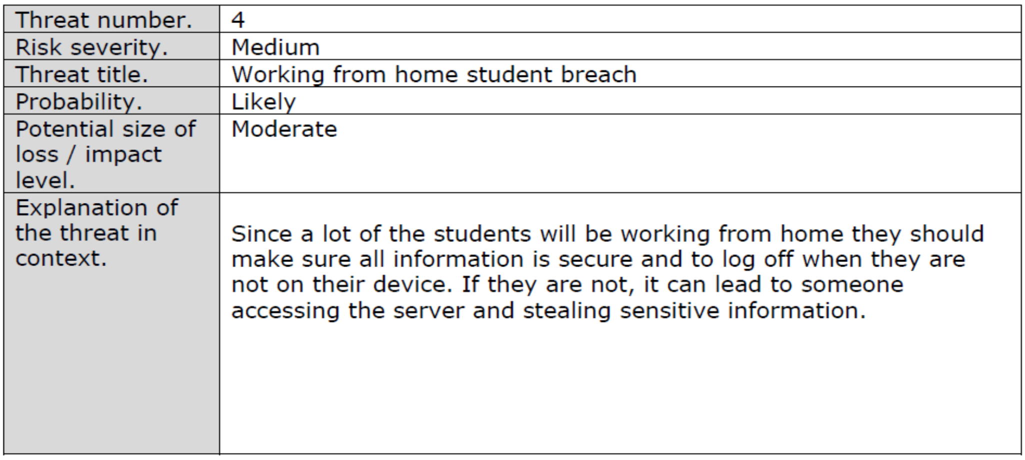
The first example shows a poor usage of the template, with an ill-defined threat, incorrect use of the threat matrix, and vague/incorrect wording for the explanation.



Threat number.	1
Risk severity.	High
Threat title.	Hacking
Probability.	Likely
Potential size of loss / impact level.	High
Explanation of the threat in context.	Someone may be able to walk into the server room during the day when the room is unlocked, and access the server, and potentially access information such as IP Addresses, and such. Not only this, but they may also be able to upload a virus whilst in the server room. To prevent these possibilities the server room must be locked at all times with only the people who require access to the room being allowed in. additionally all ports on the server should be closed.

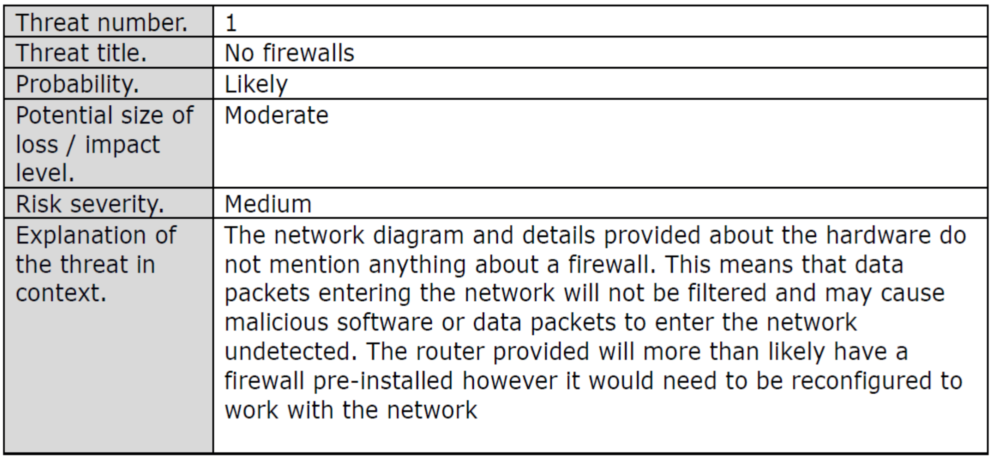
An inability to complete the template correctly is likely to affect on the Technical Language mark and may also lead to poor planning for subsequent activities.

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 ‘unattended devices with remote access facility’.



Threat number.	4
Risk severity.	Medium
Threat title.	Working from home student breach
Probability.	Likely
Potential size of loss / impact level.	Moderate
Explanation of the threat in context.	Since a lot of the students will be working from home they should make sure all information is secure and to log off when they are not on their device. If they are not, it can lead to someone accessing the server and stealing sensitive information.

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



Threat number.	1
Threat title.	No firewalls
Probability.	Likely
Potential size of loss / impact level.	Moderate
Risk severity.	Medium
Explanation of the threat in context.	The network diagram and details provided about the hardware do not mention anything about a firewall. This means that data packets entering the network will not be filtered and may cause malicious software or data packets to enter the network undetected. The router provided will more than likely have a firewall pre-installed however it would need to be reconfigured to work with the network

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, malware, trojan, worm, 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.

Measure 6 **– Enforce access rights to network based on account**

Threats Addressed

Accounts improperly configured on PCs.

Details of action(s) to be taken

Network accounts are to be given to the PCs which determine what they are able to see on the network. The admin PC for example will be able to access the admin server and configure settings there, this server will determine how access rights are configured and send data to these accounts based on their own privileges.

Devices connected to the WAP should not receive any network rights beyond internet access.

Reasons for Actions

To ensure data and network security across devices.

Overview of constraints – technical and financial

This system will be technically constrained by the need to create and configure accounts for each level of access.

This system will not be financially constrained as the software to perform this can be acquired with a free software licence that does not require purchasing to function.

Overview of legal responsibilities

Legally the network should not provide any account with data they are not authorised to see or have no reason to see, this falls under GDPR.

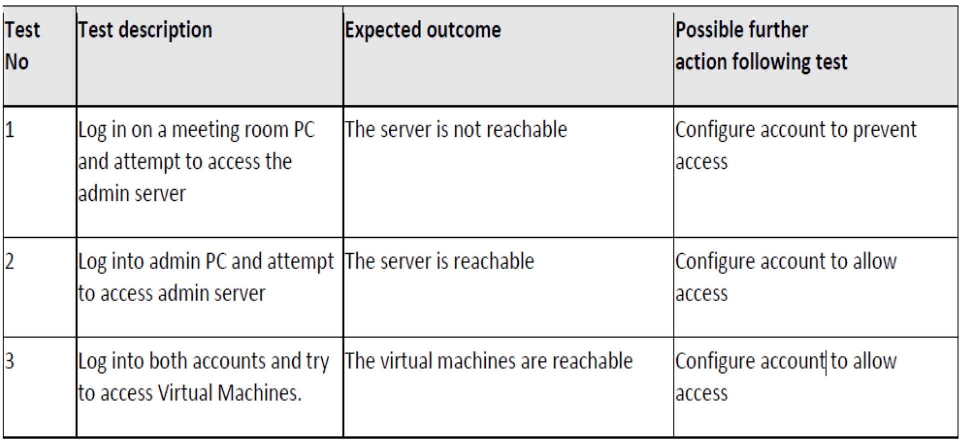
Overview of usability of the system

This should not affect the usability of the system as users will be able to access what they are supposed to be able to. The usability should only be limited in cases of attempted misuse which would fall under the Computer Misuse Act.

Outline cost benefit

There is no requirement that this solution costs any money to implement and use. For this reason I believe that the solution is more than worth the investment to create it.

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	Log in on a meeting room PC and attempt to access the admin server	The server is not reachable	Configure account to prevent access
2	Log into admin PC and attempt to access admin server	The server is reachable	Configure account to allow access
3	Log into both accounts and try to access Virtual Machines.	The virtual machines are reachable	Configure account to allow access

The next example, although addressing a reasonable situation, poor security inside the building, shows that the learner has not understood the scenario. The task brief clearly states that Projet Serendipity (PS) does not have much money and that the owners of the building, PEFER, do not want to change current security measures.

The learner has also confused PS with PEFER in the final sentence.

A more sensible and much cheaper solution would have been to change from having PS's rooms unlocked at 07:00 and then left open during the day, to having PS's rooms left locked unless a PS member is present.

1) Threat(s) addressed by the protection measure: Threat 1 – Lack of security on 2nd floor (RFID key cards, CCTV)

2) Details of action(s) to be taken: Currently there is a concerning lack of security systems put in place on the 2nd floor where PS will be housed. It would be beneficial to implement CCTV cameras in the corridors and have biometric scanners put on the doors of the admin and server room instead of the simple mortice locks which they currently have. The use of biometrics would be safer than doors being left unlocked the way they currently are.

3) Reasons for the actions: Currently the doors to the admin office and the server room are left unlocked. Alarms are only set up on doors and windows outside of opening hours meaning unauthorised access could be easy. Key cards will mean only those with permission can gain access to the protected areas, the RFID will protect them against theft too such as the admin office and the server room. CCTV will pick up anybody attempting to break into the rooms. Implementing CCTV and key cards will make it significantly harder for unauthorised access to occur which will also prevent theft of electrical equipment or data loss/theft.

4) Overview of constraints – technical and financial: Implementation of CCTV cameras and RFID key cards should not interfere greatly with the day to day function of PEFER. Implementation should not take too long and should be fairly easy to install meaning the technical constraints are mild. Financially PEFER are likely to find the implementation of these systems incredibly taxing as they are a non-profit organisation and do not have much money.

Other common misunderstandings were:

1. Thinking that PS was a business with numerous employees rather than a non-profit organisation being run by academics on a part time basis.
2. Thinking that PS was a normal school or college with large numbers of teachers and students at the premises.
3. Thinking that Linux is less secure than Windows.
4. Thinking that a clash between PS's WiFi and PEFER's WiFi is about logons or sharing a WAP, rather than what channels the two systems should be using.

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:

Professor Fred Gorse is an expert in artificial intelligence.
Professeur Adele Lefebvre studies complex data processing.
Fred and Adele are experts in their own subjects but are inexperienced with cyber
security.

This, together with other information in the scenario indicates that Fred and Adele are likely to understand technical terms but are probably not experts on cyber security language and that the report 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.

The following extract shows a good example of a management report. Note that the spending of money / misunderstanding the scenario, does not impact the assessment of this activity since the learner is reporting correctly on what they have decided in activity 2.

Management Report

Introduction

In this report below I will be discussing each of my protection measures which are included within my security plan for Projet Serendipity. I will be discussing how appropriate my choice for Projet Serendipity are, considering any alternative protection methods that I could have used and finally discussing my rationale for choosing the protection measure over the alternatives.

1 –Up-to-date Hardware

Assessment of the appropriateness of your protection measures

This protection measure is appropriate for PS since an overhaul of the equipment would increase the productivity and security of the information and data they would be producing. This is especially important from PS since they are dealing with AI and complex data processing so they will need powerful and new systems to be able to work effectively and security is essential in research so their findings do not get stolen.

Consideration of alternative protection measures that could be used

An alternative protection method that could have been used was either manually updating all of the software on the systems to the latest version that was supported. Another alternative method that could have been used was replacing the devices slowly overtime with extra subscriptions and grant money by prioritising the hardware that needed to be replaced first.

Rationale for choosing your protection measures over the alternatives.

I chose my protection method over the alternatives because I believe although it may have financial impacts on PS it is the best method to ensure the highest level of security and performance because the devices they currently have may only be able to support one or two more updates before they will no longer work and would require a new device or risking the system becoming vulnerable to attack.

The next example is an extract from a much poorer report. The learner has not laid it out well and each paragraph is a single sentence, making it difficult to read and understand. This will affect the Technical Language mark.

Report 1 on plan 1

Appropriateness of my protection measures,
My protection measures for plan 1 in upgrading the hardware and software to the latest version is appropriate because it will be the most secure way in making sure that the operating systems software is up to date and more reliable against attacks from viruses and the hardware upgrade is appropriate because it will ensure that they get the latest technology which is more reliable and is still supported by the manufacture so you can get support and warranty on it.

Alternative protection measures that could be used,
An alternative protection measure that could be used is just adding an antivirus to the operating system and making sure there is a reliable firewall ready to block any attacks on the old software and for the hardware you could get it regularly serviced to make sure it still runs as it should.

Why my measure is better than the alternatives,
My measure of upgrading the existing hardware is and software is better that the alternative method of getting an antivirus is that you will not need to upgrade in the future as you already have the newest releases and also even with the antivirus some of the bugs and threats on the old operating systems can be exploited still even with an antivirus so upgrading will still be the most secure option even with the hardware it will end up being cheaper in the long run rather than being serviced all the time and parts being changed.

<u>Task B</u>

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 six months later than the Task A scenario, when PS was being set up.

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.

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.

Many learners realised that the incident hinged on the WiFi. Unfortunately most then went on to say that it must have been an inside job, despite the fact that students had not been in the building and the PEFER staff were a very unlikely source of the information.

A good number of learners made too much of the router pinging an address at 02:00 each day. The fact that there was no response and that all packets were lost should have told learners that this could not have been a route for stealing data.
It was however nice to see some good suggestions as to what might have been happening, e.g. automatic checking for updates, which would no longer get a response as the router was out of support.

Too many learners took the easy option of saying that the incident must have been someone in PS or PEFER taking the information, with very little justification. It is of course difficult to prove that it was not such a person but the evidence items pointed in a different direction.

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.

Failures within the Organisation

Since this attack has happened I do also blame PS for the lack of preparation and their implementations to resolve the issues from the attack.

1. Firstly the router now I know that PS doesn't have a lot of money but there are more up to date and secure routers at reasonable prices which could have been used instead of this one but instead they used the router which has been out of date and out of support since 2015 meaning their network security was more vulnerable to an attack.

2. Secondly Adele only raised the matter at the next board meeting which was two laters meaning the board didn't know till only two days later which was fundamentally pretty slack. Thirdly their WAP hadn't received any patches since the system was set up which was pretty poor management as well.

3. The WAP seemed to have missed out on patches since 2017 when the system was first set up which was poor too.

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

Projet Serependinity Incident Management Policy

From viewing the policy first of all I find and when looking over to it that it is not the best and most professional incident policy I have ever witnessed or seen, there are a lot of things which can be improved in this document or policy which was being used by the firm. To start off with the positives of the document, the document does explain like it should the procedures that need to be done or carried out if and attack does take place. It covers the different methods of breaches of security within the organisation such as Theft of computer equipment, Theft of PS data which includes that the data should be backed up e.t.c, unauthorised access to PS systems and Infection of PS computer systems with malware. This document also explains the way in which the evidence is handled and kept and what the evidence will be for which is basically a report or detailed documentation of the incident from the first report to the final solution.

But then the negatives of this policy, Firstly this document doesn't actually explain how much time should be taken by the CSIRT to review the incidents as the longer it will take the more data or equipment could be stolen from them until the problem is identified and relevant security and controls is installed onto where these attacks and thefts are coming from and at what time.

Secondly at the top of the incident of the policy at the incident management policy team it says incident can be reported to a member of the Projet Serependity board which contains PhD students and supervisors so it doesn't actually give guidance to the employee who to report it to as they could report it to any student who isn't even in the board and who has no clue what so ever about cyber security.

Thirdly it doesn't actually state what can be done to prevent these procedures from happening only to report them to the CSIRT who will launch an investigation and then some considerable time later will repair the problems

- a section on recommendations

Recommendations For Projet Serendipity

For the network/Current Setup firstly this NETGEAR ProSAFE WAC730 using 802.11ac should be threw in the bin and upgraded to a more up to date and supported router such as a cisco 690 router as it will mean the network is more secure and less vulnerable to an attack. They could possibly upgrade their computers to if they wanted to but they don't have very much money so they may not be able to do this but I would definitely advise them to upgrade the insecure outdated router which is currently being used. For the wap then I would have recommended that the password was changed and that the relevant updates/patches were installed on it but Anton had already this done

Then with the incident management policy there are a lot of recommendations which are needed in this document and should be implemented and changed

1. First of all putting in a specified time limit into how long the Investigation team will be allowed to have to gather evidence and analyse the evidence and to implement a fix e.g. 7 days.
2. Another recommendation is clarifying in the Projet Serpendity Board people on the board who can be contacted as it doesn't say E.G Louise Graham, Brian Reynolds e.t.c as the board is made up of some students and supervisors so the incident could be reported to someone who isn't on the board.
3. Another recommendation could be putting in procedures to instantly stop these attacks from happening for any longer as it will stop the organisation from losing any more valuable assets or data.
4. When the theft of data happens the staff should automatically be made to change their passwords if an attack/hack takes place.
5. Having a clear leader on the investigation team as in the current policy/document it doesn't state who the leader is it only says who to contact.

Less good answers had a mixture of mistakes, statements about the system, and possible solutions. There was often no clear structure to the report. e.g.

Security Report

To prevent a similar security incident in the future a few things must be considered. Firstly, the router should be replaced with a new supported model. This is because the current router is unsupported since 2017 meaning it has missed 2 years of updates so it is not protected against some malware and hackers that can abuse this vulnerability. It is a huge security risk to the network and computers at PS. The replacement router shouldn't have a wireless connection because wireless connection can be used to gain access to the router outside of the building and inside without the permission of the PS employees. The connection should only be gained with Ethernet cables to the computers. If a mobile connection is wanted then a Wi-Fi router could also be purchased but shouldn't be connected to the business network. The password on this new router should also be stronger in case someone tries to connect their device to the router with an Ethernet cable. The password should contain: a capital letter, a number, a symbol and at least 10 letters. The password shouldn't be as simple as "project2019".

Secondly, the cleaning staff shouldn't be the last ones to leave the building while unattended. It is possible for the cleaning staff to be looking at and hard copies of documents that are being left out of cabinets by mistake. They could then leak the information that they see online which could be devastating for the business if it has personal data on it. As of now the staff can also use the router to login to the network if they can get the insecure password of "project2019". This is another way for them to leak the data.

Thirdly, students shouldn't be allowed into the building at all time. This is because they can also look at any documents that have been left out and access the network with the current router. They can then leak the data online and cause the business major backlash.

Fourthly, employee sabotage is also another issue. All employees shouldn't have access to sensitive data. This should only be accessed by employees who need it for their job. To fix this, user authentication should be added into the network so that if they want to view sensitive data they must use a second login on the network to access it.

Fifthly, a firewall must be purchased and running at all times. As a firewall presumably wasn't running before and during the incident occurred the way the data may have been accessed was through hacking. The firewall would stop the threat of hacking as long as a port scan is regularly run to shut ports.

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. It was obvious in some Task A scripts that the learners had simply used prepared statements about threats from the January paper
- 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

Ofqual

Llywodraeth Cynulliad Cymru
Welsh Assembly Government

For more information on Edexcel qualifications, please visit
http://qualifications.pearson.com/en/home.html

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

cea
Rewarding Learning