L3 Lead Examiner Report 2001

BTEC

January 2020

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_2001_ER
All the material in this publication is copyright
© Pearson Education Ltd 2020

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 (20158K)

Grade	Unclassified	Level 3			
		N	P	M	D
Boundary Mark	0	14	28	44	60

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

It was clear from the scripts seen that the majority of learners were able to understand the scenario and produce the required documents. A small number however produced responses which were clearly derived from the first SAM.

Too many others had learned generic responses. These learners seemed to be unable to adapt these responses and included generic threats and measures which had no relevance to the scenario.

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

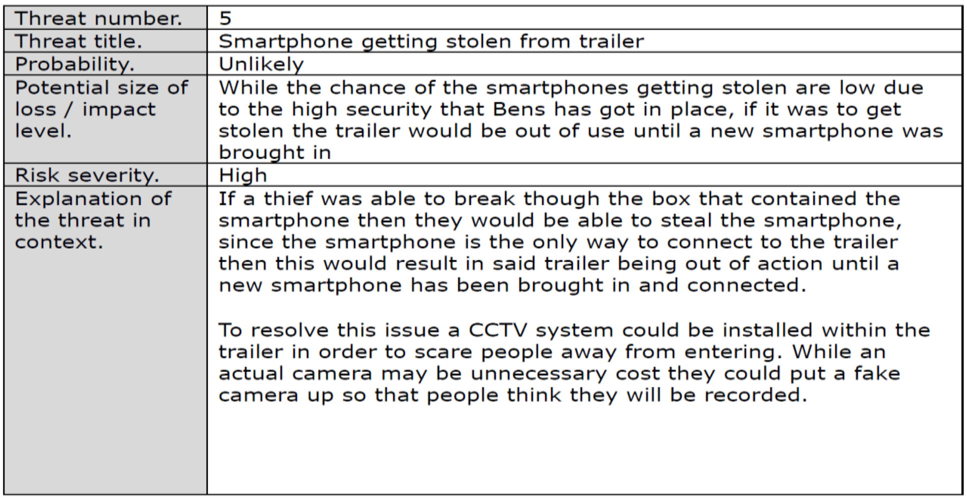
Task A

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. This often applied to an entire centre, showing a weakness in preparation.

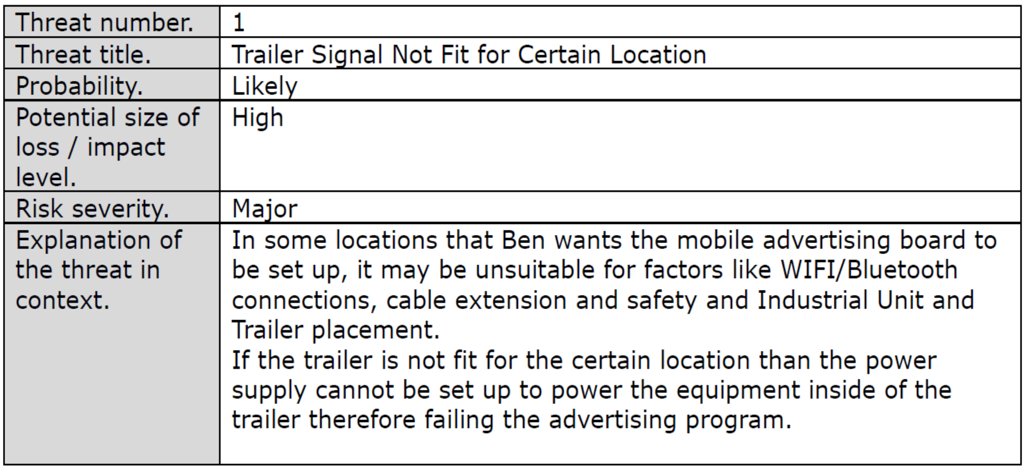
The first example shows a poor usage of the template. The threat is plausible but the pairing of the probability, unlikely, and risk severity, high, cannot be obtained from the risk matrix. The learner has also failed to give a value for the potential size of loss.



Threat number.	5
Threat title.	Smartphone getting stolen from trailer
Probability.	Unlikely
Potential size of loss / impact level.	While the chance of the smartphones getting stolen are low due to the high security that Bens has got in place, if it was to get stolen the trailer would be out of use until a new smartphone was brought in
Risk severity.	High
Explanation of the threat in context.	If a thief was able to break though the box that contained the smartphone then they would be able to steal the smartphone, since the smartphone is the only way to connect to the trailer then this would result in said trailer being out of action until a new smartphone has been brought in and connected. To resolve this issue a CCTV system could be installed within the trailer in order to scare people away from entering. While an actual camera may be unnecessary cost they could put a fake camera up so that people think they will be recorded.

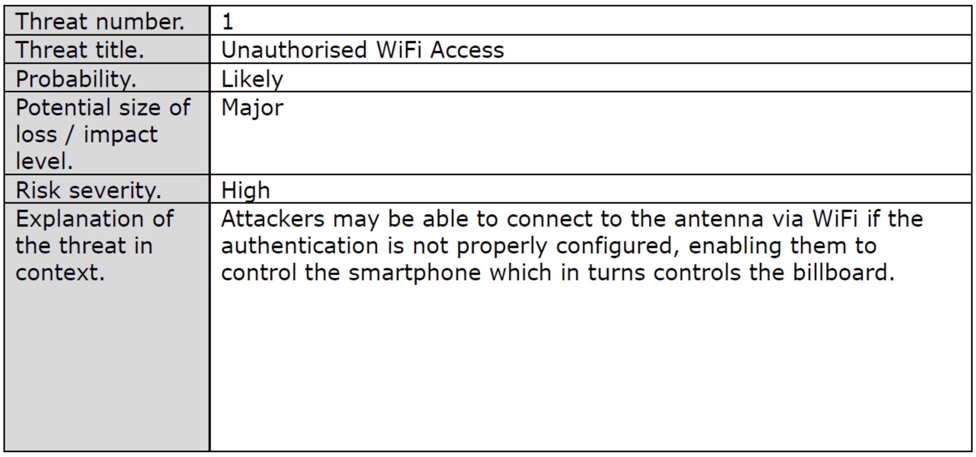
An inability to complete the template correctly is likely to affect on the Technical Language mark and may also lead to poor planning for subsequent activities.

The next learner uses the matrix correctly but does not clearly identify the threat. The explanation helps a bit but is still rather muddled. The learner has tried to cover too many ideas in one threat. WiFi and Bluetooth could perhaps have been kept together but the extension cables have little in common with them and the Industrial unit has nothing to do with the trailer.



Threat number.	1
Threat title.	Trailer Signal Not Fit for Certain Location
Probability.	Likely
Potential size of loss / impact level.	High
Risk severity.	Major
Explanation of the threat in context.	In some locations that Ben wants the mobile advertising board to be set up, it may be unsuitable for factors like WIFI/Bluetooth connections, cable extension and safety and Industrial Unit and Trailer placement. If the trailer is not fit for the certain location than the power supply cannot be set up to power the equipment inside of the trailer therefore failing the advertising program.

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



Threat number.	1
Threat title.	Unauthorised WiFi Access
Probability.	Likely
Potential size of loss / impact level.	Major
Risk severity.	High
Explanation of the threat in context.	Attackers may be able to connect to the antenna via WiFi if the authentication is not properly configured, enabling them to control the smartphone which in turns controls the billboard.

Other common errors were:

- the identification of non-cyber security threats such as multiple ways of damaging or vandalising the trailer. One instance of this would be appropriate but having damage to locks, hinges, lid, etc. 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.
- 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 enough 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 Addressed – 8,10. Weak passwords and misconfigured access rights
Actions to be taken:
Set a password policy that requires uppercase, lowercase, symbol and a range of character
Two factor authentication
Consider use of biometric authentication
Add expiry date to all user's accounts, lasts a maximum of 1 year
design management system, clear who has specific access rights

Reasons for actions:
Help prevent unauthorised access, strong password biometrics and two factor authentication help prevent unauthorised access from hacker.
Ensures users have appropriate permissions for their account, expiry date ensure users don't retain access past the date they should have access to the system which is an additional fail safe for if they forget to remove a user

Constraints:
Technical:
High – setting up and retaining user's biometric information can be complicated if you have no previous experience, especially considering GDPR and retention of personal and sensitive information.
Setting up password permissions and two factor authentication is also a small task that is required but you don't need any specialist to do so
Configuring the user permissions should be easy because the am has been built by ben. However, specialist knowledge may be required to edit the database and application to make this possible.
Financial:
Medium - May need to employ a specialist which could be costly
He does already have a knowledge of his own database and application

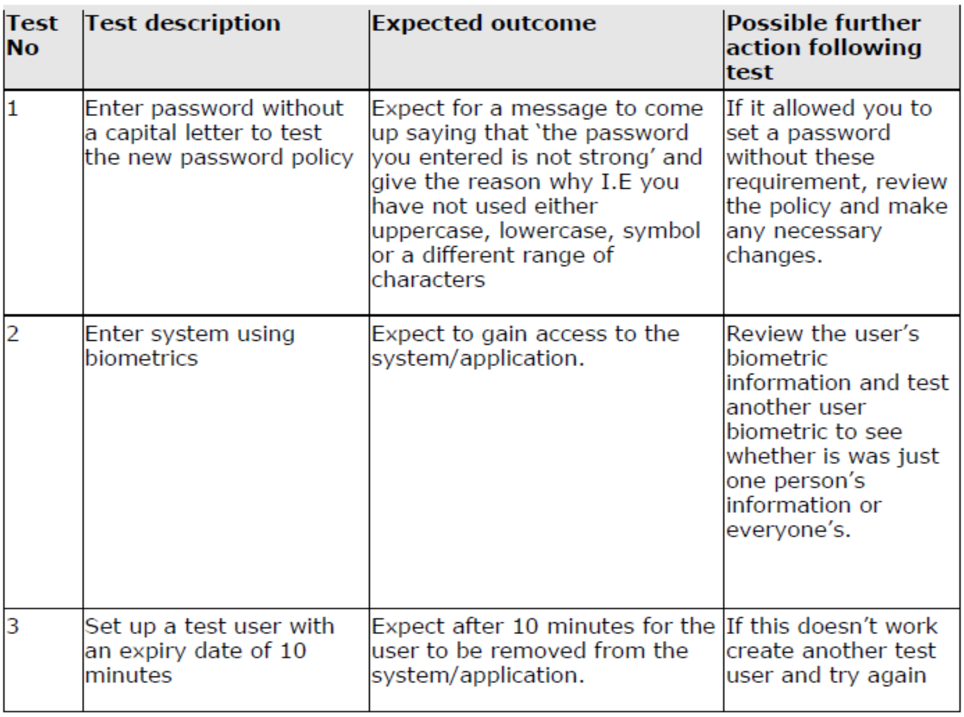
Legal responsibilities:
Ensure that he follow the standards of the GDPR.
Needs to make sure only authorised people can access client and employee information.
Doesn't retain information longer than required so this why ben will set a expiry date to ensure he is following GDPR

Usability – Medium

Every mobile phone will allow the new implication of a strong password and two factor authentication. However not all phones have to capabilities for biometrics, limiting the protection for some users.
A users account may expire whilst the account is still operational if the permissions are set wrong.

Cost – Benefit – the cost off setting up biometrics and amending the data base to add in the expiry date may be high. However, the prevention of potential data loss should outweigh this.

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	Enter password without a capital letter to test the new password policy	Expect for a message to come up saying that 'the password you entered is not strong' and give the reason why I.E you have not used either uppercase, lowercase, symbol or a different range of characters	If it allowed you to set a password without these requirement, review the policy and make any necessary changes.
2	Enter system using biometrics	Expect to gain access to the system/application.	Review the user's biometric information and test another user biometric to see whether is was just one person's information or everyone's.
3	Set up a test user with an expiry date of 10 minutes	Expect after 10 minutes for the user to be removed from the system/application.	If this doesn't work create another test user and try again

The next example, although addressing a reasonable situation, remote access to a LAN, shows that the learner has not understood the scenario. The task brief clearly states that the system will be based on trailers in remote locations, not as part of an event LAN.

Ben's system uses a trailer that can be set up at advertising sites and then operated locally or remotely in a similar way to the event systems. Each trailer will have a standard set of equipment.

The learner could have written a similar protection measure about remote access to the LAN at BB's industrial unit.

Threat addressed by the protection measure
The threats identified here consist of the threat of malicious individuals accessing the local server via connecting to the event LAN and remote access methods.

Risk severity Medium & Medium.

Details of actions to be taken
Measures that can be acted upon will consist of utilising a strong password for the event LAN, whilst ensuring it is private, rather than public. Measures for the remote access methods may include conducting an alternative risk management procedure.

Reasons for the actions
The strong password as well as the change from a public connection to a private connection will result in malicious individuals being unable to access the event LAN, therefore being unable to conduct any damage or gaining control over equipment. The alternative risk management procedure can be taken place to remove the risk of remote access by entirely removing the ability to utilise remote access in order to obtain control over the material displayed in event.

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:

Ben has more than five years' experience in setting up and securing digital information services for events.

This, together with other information in the scenario indicates that Ben is likely to understand technical terms and to have a reasonable knowledge of cyber security terms. The report should be accessible to a non-specialist but could contain some more technical language than has been appropriate in previous examinations.

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. Note that the second item, guests on the LAN, and the third item, staff WiFi, show a misunderstanding of the scenario. This does not impact the assessment of this activity since the learner is reporting correctly on what they have decided in activity 2.

1. Protection Measure 1: Changing and hiding the Blue Tooth Name / SSID
The reasons I believe that this is an Appropriate protection measure is that it ensures the security of the Smartphones in the trailers in which people externally can't see the

available blue tooth connection.
This means that they won't be able to connect to the smart phone via this method.
An alternate protection measure would be to put a very lengthy and difficult password that would take years to crack, but due to the fact that blue tooth has very bad security to begin with I made the suggestion to hide the Blue tooth name completely.
I believe that this is the most rational protection measure over the alternative, reason being that it ensures its security which is very poor to begin with as Blue Tooth can be easily hacked and spoofed, this way ensures the person doesn't even know the connection exists.

2. Protection Measure 2: Separating the staff and guests onto different virtual Lan's.

I believe this is an appropriate and necessary measure to ensure in the main office / industrial building the safety of valuable data and would eliminate the threat of guests being able to monitor the network through software such as Wireshark and possibly spoof usernames and passwords and to intercept packets of data which could contain sensitive information, and if those details got out you would be looking at very heavy fines under the Data Protection Act 1990 and GDPR 2018.
An Alternative would be to use a security captcha with terms and conditions stating that all activity would be monitored, and keystroke would be recorded so the company know who did what and when.
However I feel that my suggestion to put them on separate Virtual Lan's is far more effective in the long run and makes the sensitive data stored on a separate part of the network not be able to be known by devices on the Guest Side of the network and is a much better way to distinguish and monitor them even if it costs money to setup and to pay for the required hardware I believe it would be a worth while investment.

3. Protection measure 3: Hide the Staff Wi-Fi SSID.

I believe this is another appropriate measure to ensure the security of the network overall as if the staff network is hidden from the public it makes a lot harder to target leaving it less vulnerable to attack via Wireless methods, they would still be able to get onto the network through guest but guests are heavily restricted on what their privileges are and cant see the staff side of the network due to being on a separate Virtual Lan.
Another alternative would have been to give the staff network a very long and tricky password to crack this may seem simple, but passwords can take months or years to crack even for top of the range computers / Laptops.
However, I think my suggestion to just hide the SSID is a lot simpler as all you have to do is press a button saying "Hide SSID" in the router config and apply it and then from the public it just disappears. It also means that your staff will be able to use a simpler password without you risking the staff side of the network as to most devices it simply doesn't exist.

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 time but in a different location.

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.

In the second evidence item, Hakeem's report, Hakeem gives four possible ways in which the attack may have happened. Weaker learners should have been able to select one way and provide some supporting evidence, apart from Hakeem said so.

Stronger learners realised that the ways given by Hakeem are not the only possibilities.

A good number of learners made too much of the WiFi logs. Many of them identifying Unicorn2 as the attacker purely on the basis that they appeared on both logs. More astute learners realised that a failed login attempt does not prove guilt and that the WiFi logs would need a longer time span to be more useful.

Common errors were the assumption that the Fair HQ was only occupied by BB and that the event network had no firewall, antivirus, etc.

There is no absolute, correct answer, but the evidence points to a Bluetooth attack carried out from outside of the fence, with the additional possibility of an attack over the event LAN. The latter would also implicate a member of the event staff as the culprit.

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.

The Fair HQ was left unattended when Charita left to go to the ticket office. The HQ has devices such as the admin laptop and server that could be accessed by someone unauthorised and lead to losses in sensitive data.

- More extensive logs of the WiFi connections should have been saved. Charita only managed to save the previous 10 minutes and the investigation would be more complete if logs from before this point were also saved. Hakeem in his report assumes that there is no way to access the projectors from the public network, but this is still possible and he should've retrieved public WiFi logs from before the 10 minutes anyway.

- Hakeem only talked to one stallholder about the possibility of physical access to a projector's control box. He should have asked more witnesses about the event on the off-chance that the first stallholder was lying or wasn't telling accurate information.

- Logs should be kept for local bluetooth links to any projectors. This would allow the investigation to conclude if bluetooth was the intrusion method.

- Hakeem did not decide to contact the police after the incident. Even though there's thought to be no risk of data protection implications, the police should still be contacted after an incident like this. They could have helped find the culprit and prevent it from happening again.

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

Adjustments to the cyber-security documentation:

(a) Theft of IT equipment
i. 'Find My Device' software or any other form of tracking software is to be installed on all devices used at the fair. This allows for evidence, such as a devices last known location, to be collected; this information is to then be handed to the police to aid them in their investigation.

ii. If sensitive data is stored on a stolen device, a hard-drive wipe is to be carried out to protect this information from theft.

iii. If this isn't applicable, a password change is to be conducted remotely.

iv. Eyewitness accounts of equipment theft are to be collected to help support with any investigations.

v. CCTV footage is to be reviewed.

(b) Theft of company data

i. The ICO must be contacted, because there may have been a breach in the Data Protection Act.

(c) Infection of company IT systems with malware

i. An anti-virus scan is to be conducted on the entire network. Any further traces of malware will then be routed out.

ii. The investigation will research into what damage the malware file has conducted.

(d) Unauthorised access to company systems

i. An immediate password change is to be carried out on all relevant devices; such WAP's or staff computers.

ii. Eyewitness accounts of unauthorised access are to be collected to help support with any investigations.

iii. CCTV footage is to be reviewed.

- a section on recommendations

One improvement that I would make to the security measures is I would make sure that if there is public WIFI they should only have limited time with the WIFI this is because it would lower any chance of their being an attack from being carried out within the system and any devices that are connected to the system. Doing this will also mean that people will spend less time on their phones and encourage them to go looking round the fair and enjoy what is there.

Having looked at the network diagram I would make sure that there are different switches which have devices connected to them, this means that there will be limited access to certain devices, for example there should be a switch for the HQ and it should also include the projector control device so that the projector cannot be changed and any displays should also be connected to the same switch, and there should be a separate switch for the wireless access points as this will lower the chance of someone gaining access to multiple devices that are at the fair such as the projectors.

Also looking at the map and the way that the fair has been arranged, the projectors should be in the marquee, this will stop anyone from being able to gain access to the projectors because they will be in amongst a crowd of people where they will be seen carrying out the attack that is why the projectors would be better placed in the marquee so it makes it harder for an attack to be organised and carried out. The HQ should also be placed within or next to the marquee this will make sure that they will always have quick access to their equipment that they have got set up within the fair so that if anything does go wrong then they are able to quickly deal with the situation that they find themselves in.

Another improvement that I would make to the security measures is make sure that stronger passwords are set up and should only be obtainable by asking a

member of the BB staff that are on site within the fair this will help to lessen the risk of any unauthorised person being able to gain the WIFI password and gaining access to the WIFI itself because if a hacker gained access they would have access to lots of people's devices and could take private information from the devices and use it for their own gain. Another improvement that I would also make so security measures is have a personal from the incident management team present at the fair, this could help to prevent a similar incident from happening again because they will be able to deal with the attack or something of a similar nature whilst at the fair, the incident management team personal may be able to fight the attack whilst it is happening and find a source of where the attack originated and stop the attack from carrying out and completing its function.
I would make another change to one of the security measures and that would be the Bluetooth connectivity of the projectors, I would make sure that any Bluetooth connectivity is removed I would make this change because it eliminates an immediate source of intrusion and access into the network of various devices that are set up around the fair, this means that it would lessen the chance of an attack from happening and would make the fair safer and could help to protect valuable data that is stored on the network through the various amount of devices that are connected to it.

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.

Firstly, to avoid similar incidents, it's best to start with the mistakes and vulnerabilities found in each evidence item and then list what procedures should be made instantly. Although Charita had done well in producing a good account, she will need some little training as she had made two major mistakes: leaving the HQ whilst Hakeem was also away, and leaving a BB device exposed and connected. From evidence item 1, it's possible that the device was used to attack. BB should consider this and temporarily remove the device from the network. The chances are low, but the device may have had something malicious installed onto it. It can be checked for logs giving information on recent activities, and scanned for anything dangerous using software e.g. an antivirus. If suspicious activity is found, action corresponding to the information found will be carried out e.g. if the network key was cracked, then it would be due a change.
Hakeem had considered the incident to not be serious enough to call the police, however it would be logical if he were to call at least some form of security in case there were to be a follow-up attack as he is not sure how the attack was done and if there is going to be larger-scale attacks. Calling the police is a valid option. He had also assumed the attack was a "one-off prank attack" via Bluetooth, where instead he should've thought about the other 3 methods and made precautions around all of them. An attack via Bluetooth is quite likely and, luckily, this type of attack can't harm the company much further. Switching to wired connection would completely remove the chance of an attack happening like this again, however as Hakeem stated, there is the alternative where a CCTV could be implemented or a staff member could supervise since the Bluetooth connection requires short distance.

The Wi-Fi access log is due no improvements, as you cannot technically make any.

The network diagram shows that there are a few vulnerabilities. The router is directly connected to the internet, yet it should have layers of security. A simple solution could be to get a firewall, both the software and hardware, so that files from the internet will have to be filtered. I recommend doing this same suggestion with the ethernet links connecting the switch to the pre-booked devices. Either connect the ethernet into a its own firewall which links to the switch, or connect it to the router's new firewall. This only needs to be considered as other devices at the stools use the public Wi-Fi, therefore alternatives include reworking the link for non-booked devices. The chances of the attacker using Wi-Fi to control the projectors is unlikely, but still possible. This means that the entire system should be put under short maintenance until the method the attacker used is fully known, because if they had used the Wi-Fi then they would have had unauthorised access to the full system at the fair. It was not stated that any malware was put onto the system, or if data was stolen, so if the attack was done through Wi-Fi then the only procedure would be to renew the authorisation so that any details the attacker may still have is null.

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 SAM.
- 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