Pearson
BTEC

Examiners' Report
Lead Examiner Feedback

June 2022

Level 3 National in 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 programs 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

June 2022
Publications Code 20158K _2206 _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

The unit had a greatly increased entry over the last, pre-Covid summer series, but most centre's will have had the opportunity to learn from the 2201 series and should have been able to understand the requirements for submitting the work. The majority of the scripts 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

<u>Task A</u>

Activity 1 – Risk assessment of the networked system

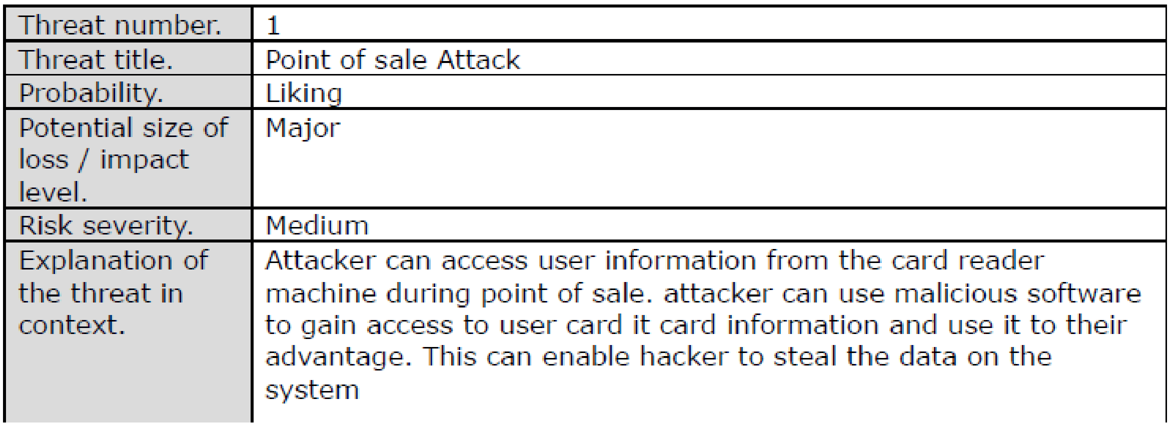
This activity requires learners to assess the cyber security implications of the scenario and produce a risk assessment. A risk assessment template is provided, together with a simple matrix for determining risk severity.

Nearly all the learners managed to fill in the template with estimates of threat probability and size of loss, but once more, a disappointingly large number were 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 centre's.

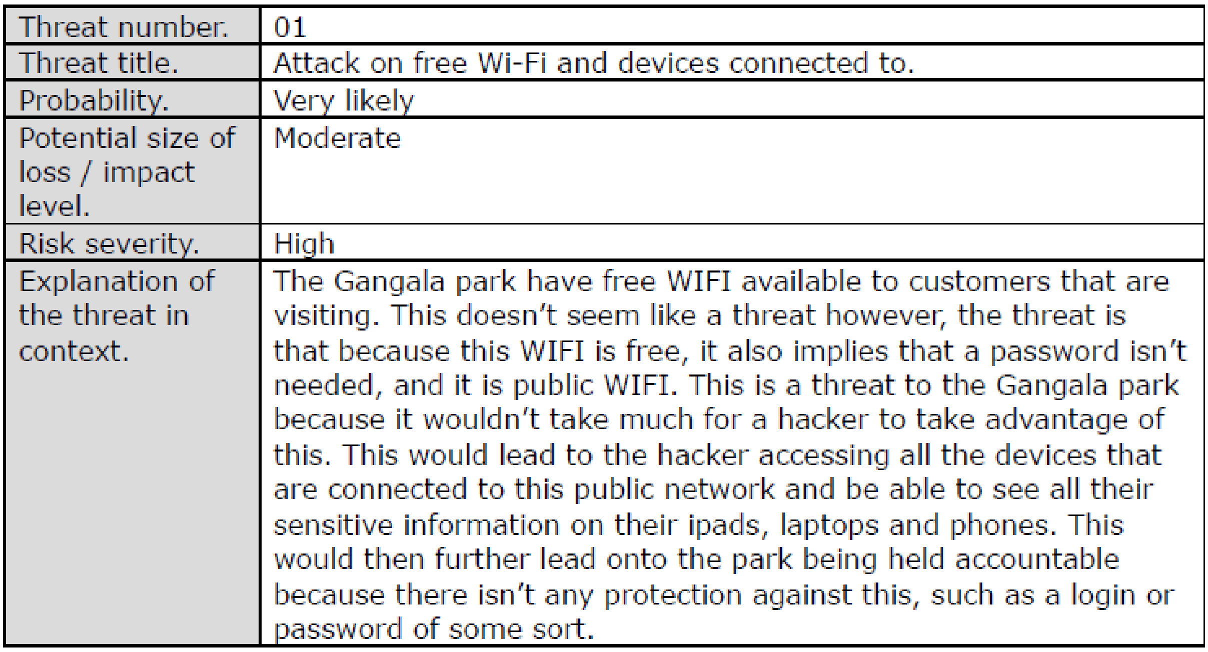
In this examination series several learners did poorly in their initial reading and analysis of the scenario. It was clearly stated that the existing system was to be completely replaced with new equipment and that the WiFi was for guests, with the staff using VoIP or two-way radios to communicate. A lot of time was therefore wasted writing about the 'staff WiFi' or the problems of 'out of date equipment'. These were presumably pre-prepared responses. Marks are not subtracted for this, but the learners were self-penalizing by using up time.

The first example is a weak, lower band 2 response and shows incorrect usage of the template. The threat is possible although the explanation is muddled and lacks detail of how the attacker might compromise the card reader. The size of loss is sensible and the spelling mistake in the probability cell is ignored. This severity value of medium is incorrect, as the matrix shows it should be high.



Threat number.	1
Threat title.	Point of sale Attack
Probability.	Liking
Potential size of loss / impact level.	Major
Risk severity.	Medium
Explanation of the threat in context.	Attacker can access user information from the card reader machine during point of sale. attacker can use malicious software to gain access to user card it card information and use it to their advantage. This can enable hacker to steal the data on the system

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



Threat number.	01
Threat title.	Attack on free Wi-Fi and devices connected to.
Probability.	Very likely
Potential size of loss / impact level.	Moderate
Risk severity.	High
Explanation of the threat in context.	The Gangala park have free WIFI available to customers that are visiting. This doesn't seem like a threat however, the threat is that because this WIFI is free, it also implies that a password isn't needed, and it is public WIFI. This is a threat to the Gangala park because it wouldn't take much for a hacker to take advantage of this. This would lead to the hacker accessing all the devices that are connected to this public network and be able to see all their sensitive information on their ipads, laptops and phones. This would then further lead onto the park being held accountable because there isn't any protection against this, such as a login or password of some sort.

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 at multiple places as separate threats is not helpful. These threats are not penalized 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.
- writing about threats to a non-existent staff WiFi.

- treating staff two-way radios as somehow being linked to the network
- fixing the Windows update problem by automatically running updates overnight, forgetting that the backup system is running at that time.

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.

1) Threat(s) addressed by the protection measure

Malware installed on Gangala Aventurparko system Threat: 11, Ransomware attack Threat: 13 and Auto execute attack on computer system Threat: 08

2) Details of action(s) to be taken

To prevent malware from being installed on the system in the first place from a memory drive the system should turn off the Auto Execute feature on window machines. The next action that should be taken is installing a type of Anti-malware on the systems. Taking a system backup quite often.

3) Reasons for the actions

The reason you should turn off the Auto Execute it will prevent programs from auto executing their selves either when installed on the system or when a memory drive has been plugged in. This will prevent any kind of program that could have some type of malware won’t run by itself unless a user runs it. This will not protect against already installed and running malware on the system. That why anti malware software should be used. The anti-malware software should have real-time scanning. This will be used to scan the system files and remove any that are malware. This will also protect against ransomware being installed. The use of a system backup is if all fails, and malware destroys all the files on the system or ransomware encrypts the files you can restore from an older backup before it happened.

4) Overview of constraints – technical and financial

You do not need a huge amount of knowledge and skills to be able to disable auto execute. There is a guide online on the Microsoft website with a step-by-step guide on how to disable auto run. There is no extra cost of turning off a feature that is already in windows.

Install anti-malware is straight forward but will take a large amount of time to do to each system. Anti-malware is very user friendly by automating a large amount of the setup part. There will be the cost of buying the software this is normally done in a subscription.

The final action is taking a system back-up often. this will require the use of the backup server and the skill to setup an automatic backing up. Restoring from a backup will require reinstall from a possible loss from when the backup was made. The park already has the equipment required to take a backup.

5) Overview of legal responsibilities

The legal responsibilities of the organisation are to protect customer data under Data Protection act 2018. If malware is installed it leads to the risk of data being stolen this may include customer data.

6) Overview of usability of the system

The system running anti-malware will be slower as the anti-malware will be always running in the background. This will mainly affect the CPU performance and take up more RAM. During a backup the computer may go even slower as the CPU performance again will drop and so will the Drive it is backing up. The system will work as before but with slightly worse performance.

7) Outline cost-benefit

The cost of backing up and having Anti-malware is far cheaper than the cost of losing data and a whole system to malware and ransomware. By being able to restore to a previous backup it will lower the down time of operations.

Test No	Test description	Expected outcome	Possible further action following test
1	Plugging in a memory drive with a video.	The video will not play automatically.	If the test fail, ensure the autorun is disabled.
2	Accessing website with malware on an isolated environment preventing further spread in case of test failure.	The website will be blocked by the anti-malware.	If the test fail, ensure malware is removed from the system and try and ensure the anti-malware is setup correctly.
3	Restoring from backup	The system will restore the version of the backup,	Ensure they are being taken and try and restore again.

The next example shows a reasonable measure, firewall, but has a limited account of where the firewall would be placed, there is already one shown on the network diagram.

The learner's answer, although using the template, also does not make it clear what the tests are.
This would be a lower end, band 2 response.

Threat(s) addressed by the protection measure

Someone could hack into the private WIFI.

Details of action(s) to be taken

They would need to install a firewall into the network.

Reasons for the actions

The main reason would be that it would be able to filter out any kind of activity that would occur like an email being sent through without the sender address being familiar. This would ensure that the security officer within the organisation will be able to see what is going on via the activity log and be able to get investigating in a safe environment.

Overview of constraints – technical and financial

They would need to install the firewall itself and they would also need to hire someone that can maintain it. This means that they must pay a lot of money to make sure that it is operating condition.
They would also have to make sure that it is installed properly as well because if done wrong, it could break something else in the system or put it in more danger.

Overview of legal responsibilities

The act would be the computer misuse act, the reason would be that the company is now able to get the necessary equipment in order to find out what the person is doing to their system and get the right punishment for them.

Overview of usability of the system

It could end up slowing down some methods of communication between the employees because the firewall would need to check if everything is safe and secure.

Outline cost-benefit

The company would need to make sure that everything is working correctly but there is smaller risk of the confidential details getting stolen. This would be good because the fine for letting it happen is bigger than the purchase price so it would be beneficial.

Test plan Test No	Test description	Expected outcome	Possible further action following test
1	Is the firewall able to check communication?	The firewall can scan each line of communication for any usual activity.	They would need to see if the café can use it as well.
2	Are the configurations all set up properly?	All the settings are properly adjusted for the network and the services.	They would need to see if they can alter it for the public services.

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. It will usually be assessed against what is given in Activity 2 but could be assessed against Activity 1 if Activity 2 is missing.

The report should be an accurate representation of the solution. If some of the ideas in activity 2 are incorrect, the learner can still get a good mark for reporting on them.

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:

Viro De Ordoni is an experienced Project Manager. He has previously managed several successful projects for VLLP. He has a good knowledge of IT matters but relies on managing other people’s expertise rather than trying to do everything himself.

This, together with other information in the scenario indicates that Viro is likely to understand technical terms but 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 an extract from a good example of a management report. It gives a problem and solution from Activity 2, and discusses an alternative, with reasons for choosing the original solution. Note that this learner has not realised the problem of an overnight update possibly clashing with an overnight backup. This could have been given as another reason for not choosing the alternative.

3. Ensuring that the windows updates on command and permission of the employees.

Ensuring that the windows updates manually and not automatically, makes sure that the system is not disrupted by the update, which means that the system will automatically be updated, and this could occur when the employees are working, which can lead to loss of data. This is appropriate because it ensures that employees can update at specific times and more flexibly.

My alternative for this measure is to update at a set time and not ask the employees, ensuring that the update is always at a set time means that the update will update only specifically to that time, for an example if the time is set to update overnight, this ensures that employees are not affected, and the system Is not disrupted by the updates whilst work is going on.

To justify I talked about my initial measure to ensure that the update happens only when the employees allow it to take place, to ensure that the system is not disrupted, and the update can be done more flexibly. In my alternative solution I suggested that the system is updated at a set time, so employees won't have to manually update the system themselves. To conclude I think that my initial measure is more effective as it ensures that the workers can be more flexible, rather in my alternative solution, the employees won't be able to access the system at that specific time the update I launched if they wanted to. Therefore, the fire solution creating more flexibility.

The next extract is a lower band 2 answer. The original measure is weak, although accurately reported from Activity 2. This is acceptable, Learners are not double penalized for a poor Activity 2 answer. Marks are however lost due to the weak alternative of using a mobile phone instead of a wristband. The learner has not understood the scenario and the limitations imposed by water activities.

3 - Theft of customer details using RFID readers or Copying of RFID chips in wristband by Fraudsters

Appropriateness of Protection Measure

Customers are told to look after the wristband as this way it can prevent this threat from occurring. As there here is no way of employees knowing whether a RFID wristband has been scanned and details have been stolen customers will be told to notify them if they do think their RFID wristband has been scanned. Encryption of RFID wristband can also take place to prevent fraudsters from getting the card details stored on the chip.

Alternative Protection Measures that Could be Used

The company should introduce contactless payment via mobile devices. This is much more secure than the RFID wristband as the user data is not at risk of being stolen using a decoder if the wristband does not have secure encryption. The company should make sure that the customer's pay via contactless payment on their smart devices such as the mobile phone or smart watch this is because when you make a contactless payment using NFC on your mobile device the user, must verify if they are the phone owner and are aware the payment is being made as the device asks for the user biometrics for approval. For example, with apple devices such as the iPhone when making a payment the user is asked to verify their identity via face ID, this is much more secure the RFID wristband as the device is encrypted via company software as well as biometrics, so the user is aware of payments being made.

Rationale for Choice of Protection Measure

I think that the best method for protecting customer security and data is to use the 2nd method of using customer own smart devices which already has encryption built into it to ensure no data is stolen as well as having further security such as biometrics to prevent the stolen device being misused by someone who is not the owner of the device. This level of security is not in the wristband, as when the wristband is stolen off someone wrist by a con artist for example, the con artist can spend the victim's money effortlessly as the wristband does not have any security to verify if the actual owner of the wristband is using it and the con artist can use the NFC and tap to pay for purchases with ease.

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 penalized 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 1, the **Team Leader's report.** Learners are told that:

The team concluded that there were three possible causes.
1. A bug in the drinks station or billing software.
2. An error in setting up the wristband chips for the customers involved.
3. An attack on the RFID identification/authorization system.

Too many learners simply took these as being the only options and didn't look any further into the evidence.
Many Learners also pre-decided an outcome, usually one of the three, and then found ways to make the evidence fit what they had decided.

In evidence item 2, **Drinks station operations report** it is stated that the range of the RFID reader was 30cm. It appears that many learners are confused as to how big 30cm is. Too many claimed that this meant the drinks station would read the wristbands of passers-by, so generating the false purchases. A relatively small minority realized that the 30 cm limit must mean that the visitor's wristbands were being read/cloned elsewhere.

Evidence item 3, **Drinks station logs**. Analysis here was often superficial. Few learners noticed that there were two drinks stations involved, although this was also stated in evidence item 1. Another error was in thinking that the blanks in the Payment Card column meant an incorrect/tampered with report, rather than a cash payment into the client's account.
Better learners were able to say that the I minute gap between the two drinks looked like normal operation of the drinks station and that the false purchase of the same two drinks on two occasions could indicate that someone was 'tapping into' RFID chips to get their codes and there were likely to be two people involved.

Evidence item 4, **Network diagram**. Although evidence item 2 states: Malfunction reports are sent to the Maintenance department via the network.
I did not see any scripts that noted that the drinks stations are not shown on the network diagram. This would call into question the accuracy and completeness of the evidence.

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:

1. A section on the mistakes made. eg.

Mistakes:

- The team leader did not follow up their word-of-mouth account with an email, this only gives the spoken account as the evidence and there is no proof that what was said, was said.

- The team leader gave their account two days after the event happened. This means that during the time after the incident the team leader could've forgotten crucial details, and this could hinder the investigation.
- The legal department decided to not follow the cyber security incident management policies and didn't appoint any representatives due to low staff members on the weekend, even though the team leader suspected that customer data may have been compromised. This is blatant disregard of the document outlining the policies in place.
- As highlighted in evidence piece 1, *Team Leader's report*, a PIN was suggested to be implemented as remedial action however the senior management decided to not implement this, leaving the RFID payment system unsecured and open for future attacks which could be identical to what was seen in the two incidents.
- The proprietary system was just left as a dead end. The team should've investigated further and contacted the outside company to follow up and ensure that it was not a bug in the system. This would then rule out that as a suspect and could've helped the investigation finish earlier.
- The RFID payment system is open to threats as there is no security measures in place. This could be in breach of data protection laws as the customer's personal and identifiable data was breached.

2. A section on the security documentation. eg.

1. The first adjustment that I would make is to the 'Incident reporting' section and I would implement a timescale in which after informing a team leader, a staff member must write and email a report of the situation and preferably this report would have to be written, at maximum 24 hours after the incident occurs. This is because the longer it takes to write the report the less accurate the information becomes due to human error and memory loss etc.

2. There is no incident management on how to deal with a situation, for example when they were trying to find out what went wrong in the first report, they did not test anything properly or write a report on the results which makes the situation a lot harder to deal with as there is a clear lack of evidence.

3. In '**Theft of IT equipment**' there is no mention of any procedure that the staff should take to stop an attacker from stealing information, for example if a hard drive was stolen then it should be remotely wiped and if this is not an option then a remote password reset should be carried out.

3. A section on recommendations. eg.

1. Implement security measures to the RFID chips to prevent cloning.

2. Have a checkup with the external organization to check over the software of the drinks machine.

3. Principle of least privilege.
• Ensure verbal accounts are made as soon as possible.
• Ensure email accounts are followed up after a verbal account and are made as soon as possible.
• Ensure incident management policies are followed to prevent further attack.
• Ensure that security measures are put in place to prevent further attacks on the organization.

As the most likely solution to this issue is that RFID cloning took place it would be the obvious thing to **implement security measures to the RFID chips to prevent cloning**. These chips are unsecured at current time and open to any attack that could happen to them. To secure the chips, the organization could look to add a two-factor authentication to any payments. This could be in the form of a PIN number, as previously spoken about – however this could also be stolen by the attacker who could just as easily enter the PIN themselves. The
safest option for the organization to take in this situation would be to implement a use of a biometric fingerprint scanner. This would mean that it could not be replicated by an attacker as the fingerprint is unique to a person.

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 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

For more information on Edexcel qualifications, please visit
http://qualifications.pearson.com/en/home.htmlPearson Education Limited. Registered company number 872828
with its registered office at Edinburgh Gate, Harlow, Essex CM20 2JE