Sample Pearson BTEC Set Assignment Brief

Single Part Assessment

Unit 11 – Cyber Security and Incident Management

For use with:

Pearson International BTEC Level qualifications in Information Technology

Foundation Diploma / Diploma / Extended Diploma

Advised supervised hours	20 hours

For completion by the centre

Qualification (select as appropriate)	Foundation Diploma / Diploma / Extended Diploma
Assessment date	

The Pearson Set Assignment will be assessed internally by the centre using the unit assessment criteria given in the qualification specification. The Set Assignment will be sampled by the Standards Verifier as part of the standards verification annual centre visit.

Conditions of supervision

The Pearson Set Assignment must be carried out under supervised conditions. We advise that the Set Assignment can be in more than one supervised session.

The Set Assignment must not be shared with learners before the supervised session that will be arranged by the centre. Tutors and invigilators should take note that they are responsible for maintaining security and for reporting issues to Pearson. In particular:

Outcomes for Submission

Learners must complete this set assignment on a computer, using office productivity software.

Learners must save their work regularly and ensure that all materials can be identified as their work.

Learners must submit their own, independent work as detailed in the set assignment.

Read the Set Assignment Information carefully.

You will be asked to carry out specific written activities, under supervised conditions, using the information provided.

At all times you must work independently and must not share your work with other learners.

You must complete ALL activities.

Set Assignment Information

You work for a new cyber security company called 'Cyber R Us' who are delivering security products and services across the entire information technology infrastructure. The company develops cybersecurity software including firewalls, anti-virus, intrusion detection and protection, and endpoint security. Cyber R Us are tasked with protecting companies' networks, clouds, web applications and emails. They also offer advanced threat protection, secure unified access, and endpoint security.

One of the clients (International Money Transfer Limited (Ltd)) of Cyber R Us has tasked the company to investigate the security implications of developing an internet-based financial transfer application, which allows people to transfer money quickly and cheaply to friends and family both at home and abroad.

The director of the company understands such a system would be the target for cyber-attacks. As you have recently completed a BTEC course which included a unit in cyber security, the director has asked you to investigate and report on potential cyber security threats to their web site and software.

Set Assignment

You must complete ALL activities

ACTIVITY 1 – suggested time 5 hours

Produce a report that evaluates the security threats to International Money Transfer Ltd and how these threats can be overcome.

The report should:
- explore the cyber security threats to which organisations are exposed and the system vulnerabilities that can affect the IT systems
- consider the impact that cyber security threats have on International Money Transfer Ltd and the relevant legal requirements
- consider how cyber security can impact on networking infrastructure and resources of International Money Transfer Ltd and the security implications of this impact

- evaluate the measures that can be used to protect International Money Transfer Ltd from cyber security threats and how effective these measures can be along with the legal requirements involved.

This activity covers learning aims A & B A.P1, A.P2, A.P3, A.M1, AB.D1 B.P4, B.P5, B.M2
No templates required for this activity

ACTIVITY 2 – suggested time 15 hours
The director of Cyber R Us was pleased with your report on cyber security threats. He would now like you to assist with one of the company's other clients, Black Country Training and Assessment (BCTAA) and investigate how Cyber R Us can help them to implement a cyber security plan. For this activity you must refer to the case study on BCTAA. Read the case study carefully before attempting this activity. You need to create a portfolio of evidence including: ● a risk assessment of system vulnerabilities for BCTAA. ● a cyber security plan for BCTAA with a justification of the security measures used to defend BCTAA. ● a report to evaluate both the cyber security plan you created and how it impacts the internal policies and external service providers. ● explore how forensic procedures can be used to collect evidence on a suspect system and evaluate the impact these can have on an organisation.
This activity covers learning aims C & D C.P6, C.P7, C.M3, CD.D2 D.P8, D.M4
No templates required for this activity

Pearson
BTEC

Case Study

Black Country Training and Assessment
Black Country Training and Assessment (BCTAA) offers vocational-based training and assessment services for small and medium-sized businesses.

The details of freelance trainers and assessors are stored on a database. This is used to pick staff whose knowledge meets client requirements.
BCTAA develops bespoke training and assessment for vocation skills, such as IT skills, the maintenance of unusual machinery or working with a unique production process.
Bespoke training requires collaboration with the client and often includes handling highly confidential information, such as trade secrets.

Full-time Training Managers meet clients and work with them to create and run bespoke training and assessment.

BCTAA is moving from a business park on the outskirts of Birmingham to larger city centre premises. The company has taken a lease on the 19th floor of a 20 storey building, Edexcelsior House (EH).

The building has mixed commercial and office usage. The 18th floor is leased by a recruitment agency. There is a restaurant and coffee bar on the 20th floor and a café in the garden on the roof. There are several small retail units on the ground floor. There is a gym, an art gallery and meeting rooms on other floors. A number of different companies have office space in the building.
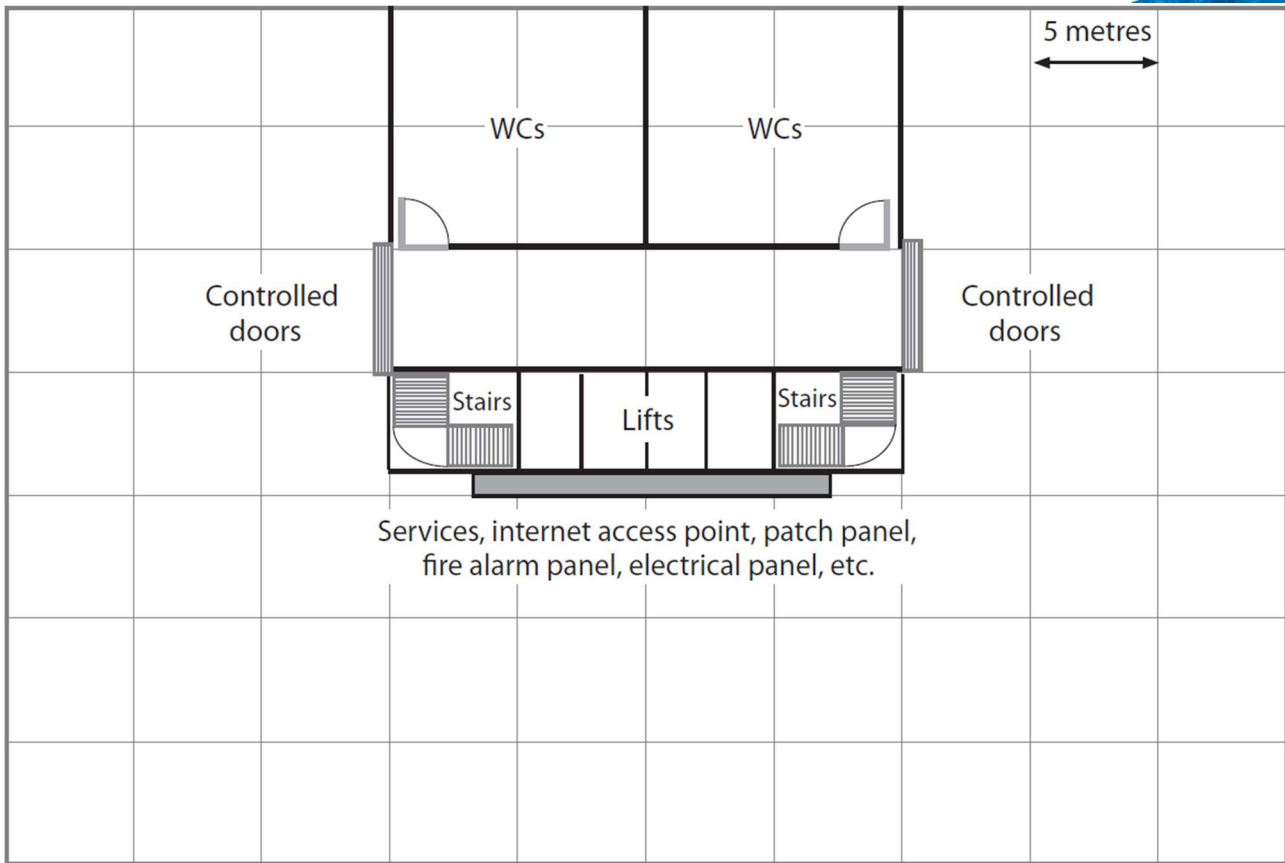
Figure 1

A plan of the 19th floor, to be leased by BCTAA, is shown in **Figure 1**.

Most of the public areas are open outside of normal office hours. The restaurant and café are popular in the evening.

The lifts, stairs, toilets (WCs) and the area around them is used by the public. The remaining area is a private, single open space that can be partitioned to create rooms or workspaces. The 19th floor has many electrical points. The data outlets have an optical fibre internet access point. The data outlets are connected by Cat6 cable to a patch panel near the internet access point. BCTAA will have to setup their own network devices.

The private area of the 19th floor is protected by a card reader door control system. This uses near field communication/proximity cards, similar to those used for contactless payment systems. The readers are already in place for each door. The EH management company supplies cards, a card programming device and logging and control software. The doors can also be unlocked from the inside by means of a push button.

BCTAA has asked you to advise them on setting up and securing its network in the new location.

Your contact is Baljinder Singh, an experienced computer user who is responsible for the current network. He is not a network specialist and says that the current system "had stuff added when we thought it was needed." Baljinder has produced a basic network design and wants you to review his ideas, and to make sure the new system is secure from the start.

Figure 2 shows the outline network diagram received from Baljinder.
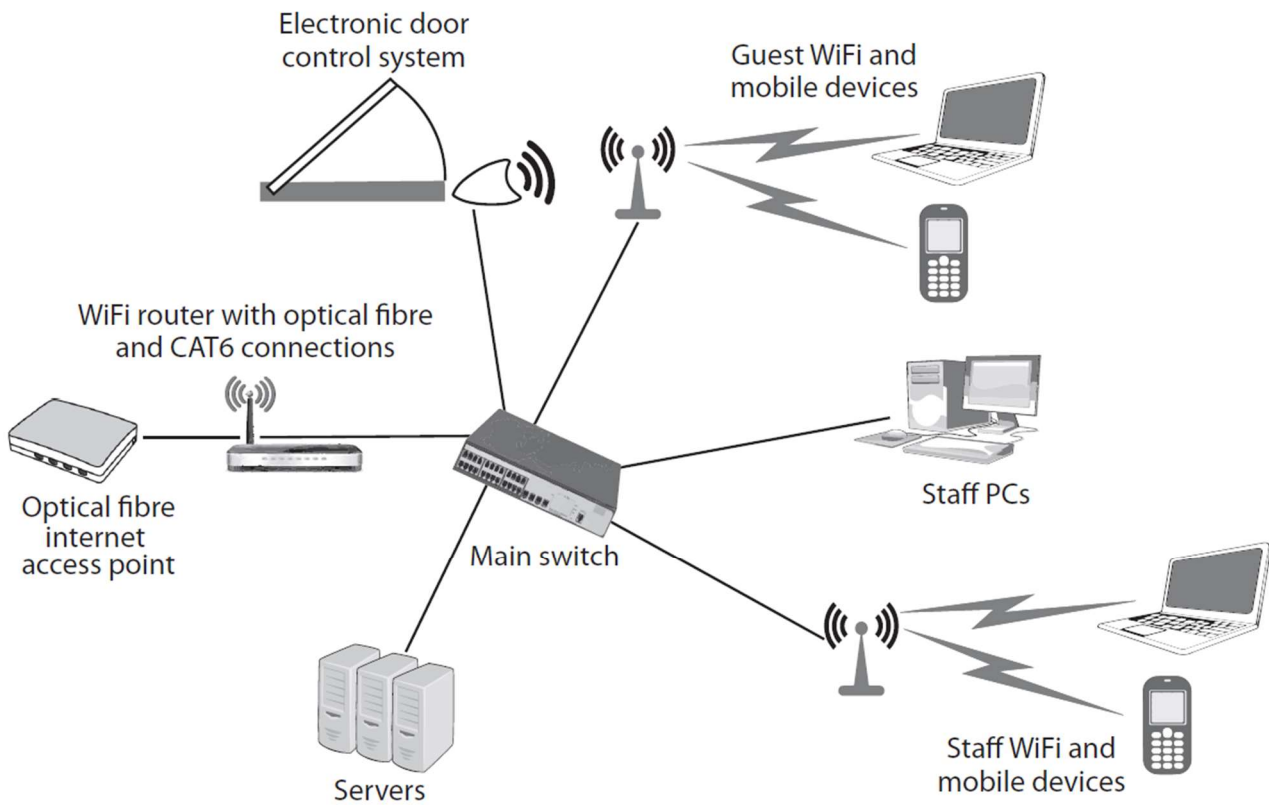
Figure 2.

Development plan

At a meeting with Baljinder, you agree these points on the development of the new BCTAA network.

1. The network will conform to the outline network diagram.
2. The network uses private, Class C, IPv4 addresses.
3. The Edexcelsior internet access system will be kept and will use a fibre optic connection point.
4. The door control system will not be changed.
5. The BCTAA network must be protected against intrusion through the internet.
6. The router must include a firewall and relevant cyber security technology to protect the network.
7. Both staff and visitors must be able to connect using mobile devices.
8. Some visitors will be clients who may need access to appropriate secure areas of the network.
9. Freelance trainers and assessors will need access to appropriate secure areas of the network from home or work locations.
10. Some staff will need access to secure areas from home or client company locations.
11. A virtual private network (VPN) will be used to facilitate items 9 and 10.

You must now create a portfolio of evidence for activity 2.