**7.1 - Know Your Threats**

**P1 – Threats to an organisation**

For this criteria, I will be exploring and explaining the threats that an ISP (Internet Service Provider) might face, including who might cause it and what consequences it would have.

DDOS Attacks  
A DDOS (Distributed Denial Of Service) is when multiple computers flood a target computer or network with traffic to deny service to users.  
Multiple computers are used as a single computer cannot output the sheer amount of data required to bring down a network. For large attacks against bigger organisations, up to hundreds of thousands of computers can be used.  
Often these are ‘botnets’, large groups of computers that have been hacked without the user knowing, and can be instructed to send spam traffic the targeted network.  
In 2015, the world’s largest DDOS attack happened, and the maximum recorded traffic flow directed at organisations was 24GB/s.  
While large server companies such as Google could handle the volume of traffic, the problem was that ISP’s connections between servers and users have a maximum bandwidth of 10GB/s. This meant packets piled up at the ISP’s servers, preventing them from providing internet for their customers.  
As well as cutting internet to customers, service that rely on the ISP could also fail, such as traffic or weather monitoring systems.  
Another issue is that the security algorithms that would usually spot a regular DOS (denial of attack service) are overwhelmed by DDOS attacks, as the data is coming from so many sources. This makes it much more difficult to identify malicious traffic, and it can slip through with the spam data. This means any users that do manage to get service have an increased risk of being hacked or infected with a virus.

Phishing  
Phishing is the practice of sending malicious code or files via an innocent-looking communication, usually email.  
If a member of staff at an ISP were to open such an attachment or link, the malicious code could infect the ISP’s server or other computers, and could destroy or steal data about customers. Some viruses can even damage hardware, which could become very expensive for the ISP to replace.

Physical Damage  
ISP’s have large server rooms that route traffic between servers and users. These servers are very powerful computers, and are usually very expensive, up to hundreds of thousands of pounds per rack.  
For this reason, server racks are kept in secure rooms, primarily to keep them cool and reduce noise pollution, but also to prevent fires and sabotage.  
Physical damage could be an internal threat – such as a disgruntled employee taking a large axe to the data banks – or a natural disaster, such as an accidental fire or an earthquake.  
Most server rooms have secured access for this reason, so only authorised can access the server room after they have been given permission. They also contain anti-fire systems, as well as redundant power supplies, and some even have measures against earthquakes.

**P2 – Information Security**

Threats to IT systems  
There are many different threats to IT systems, some of which are specific to certain systems. However, they can all be classified in one of two ways – internal or external.  
Internal threats come from inside the organization, usually from a staff member.  
External threats come from outside the organization, such as hackers.

Most threats can be either internal or external, it just depends on who is carrying them out.  
More specific categories of threats include:

* Physical threats – when hardware is physically damaged. Could be by hand, or a virus that overloads the system.  
  This also includes natural damage, such as earthquakes, fires and hurricanes.
* Hackers – people who try to gain unauthorised access to systems by exploiting weaknesses in security.
* DDOS – When the system is overloaded by traffic from many different locations.
* Viruses/worms/etc – malicious code that steals or damages data, and can even damage hardware.
* Trojans/phishing – innocent looking communications that are actually malicious, such as an attachment that gives a hacker access to a system, or tricks users into handing over confidential information.
* Packet sniffing – a form of hacking that allows the hacker to see confidential data sent between systems.

All of these threats could be from an employee – internal – or somebody outside the organisation – external.

Luckily, lots of different tools are available to help secure IT systems against these threats.

* Secured access – hardware and access points to a system are kept in locked rooms, which only authorised people can access.  
  Some datacentres also have measures against earthquakes, fires and other natural disasters.
* Authorisation systems – these are software that prevent hackers from gaining access to a system. They encrypt data and communications.
* Traffic filters – these block or ignore traffic from specific IP’s, or stop malicious packets entering systems. Firewalls can prevent certain access points being used.
* Antivirus software – this would generally be used on staff PC’s. It can identify malicious code and stop it from damaging the PC.
* Encryption – this will ensure that anybody who intercepts communications will not be able to understand them, rendering the data useless.
* Backup power – if power to the system is cut, they may have a UPS (uninterruptable power supply) or emergency power to keep the system running until a fix is found, or to give the system time to safely shutdown.

Some issues that could have an impact on security include:

* Expense – security measures against physical threats tend to be very expensive.
* Staff – most security requires multiple qualified staff that a small organisation may not be able to get.
* Ignorance of threats – again, this mainly affects small businesses, but if the owner or manager is not aware they need security they may not put any in place, leaving them open to attack.

An example of a company with excellent security is Amazon – nobody outside the organisation knows where their datacentres are, although they are reported to have military-grade onsite security. They have 99.99% uptime. It is commonly quoted that their only physical threat is a meteorite impact.