**P2 – Physical Security**

Physical security refers to protecting both hardware and software from physical threats, and using physical means to protect them.  
A physical threat is something that can damage hardware. For example, a fire is a physical threat. Another physical threat is sabotage – somebody could walk into a server room and destroy the server racks.  
Physical threats are prevented through physical security. Despite its name, a firewall will not stop a fire. Instead, fire alarms and sprinklers would be used to stop hardware from being damaged by fire.  
Another risk is sabotage. Server rooms, or anywhere that valuable hardware/software/data is stored will have restricted access, usually by requiring a key, passcode or key card to enter the room. Server room doors are often reinforced to prevent forced entry.  
One type of physical threat that is more difficult to protect against is natural disasters. Because they are varied and unpredictable, only broad measures can be taken against them.  
Data centres are usually built near the coast, as the seawater can be used for cooling. In some cases, this puts them as risk from tsunamis and floods. This can be mitigated by building the datacentre on higher ground, or on an area of coastline that is not susceptible to flooding and tsunamis.  
Inland, another natural disaster that could pose a threat is an earthquake. To reduce damage, it is possible to build server rooms with shock-absorbent foundations that automatically shut down servers when a tremor is detected, to prevent loss of data.  
The best form of protection against any kind of physical threat is redundancy. This means having backups of critical systems and data to fall back on. The simplest form of this is having multiple copies of things. This can be done with a RAID hard drive configuration, which writes the same data to multiple drives.  
A better way of backing up data is to have it copied to a drive that is then moved to another location. This could be a third-party storage service (i.e in the cloud, or a self-storage centre) or another data centre.  
As well as backing up data, it is important to have ‘backups’ of hardware, or redundant hardware. This means that when something fails or is damaged, other hardware can take over and minimise the disruption. Some organisations have redundant hardware in the same server room, while larger organisations (such as Google and Amazon) will have multiple datacentres to help distribute load.

