Physical security involves security controls on physical access to facilities. From a wiring closet to an entire office building, physical security is responsible for guarding assets from unauthorized access.

# Instructions

In this assignment, you will implement a physical security plan for a data centre building. For each of the items below, identify one potential security vulnerability and a security control to mitigate the security risk. List the type of protection it offers (deter, delay, detect, access, response, recovery), as well as your justification for choosing the technology.

* Data centre parking lot
  + Vulnerability: Public access to the parking lot
  + Security Control: Add a blocker into the entrance of the parking lot to record who comes and goes and when.
  + Protection: detect, access, response
  + Justification: By recording the people entering and leaving the parking lot, you have a higher chance of catching a malicious actor by reviewing who was there during the incident and then responding to that information.
* Building front door
  + Vulnerability: Public access to the building for potentially malicious individuals.
  + Security Control: Security Personnel / Metal Detectors
  + Protection: deter, detect, access, reponse
  + Justification: security personnel and metal detectors can detect people bringing in tools that they would need to damage or steal information from the data center, and thus prevent access. As well as the sight of the security would deter possible attackers.
* Front lobby
  + Vulnerability: Public access to different parts of the building
  + Security Control: CCTV cameras
  + Protection: deter, detect
  + Justification: CCTV cameras would be able to detect suspicious activity in public areas of the building. As well as their presence would deter potential attackers.
* Entrance into data centre area
  + Vulnerability: access to the most important and vulnerable point of the data center.
  + Security Control: Security doors/locks
  + Protection: deter, delay, access
  + Justification: By installing something like electronic locks on a security door leading into the data center area, you would prevent unauthorized personnel from accessing these areas.
* Server cages
  + Vulnerability: physical access to the servers themselves
  + Security Control: Sturdy construction to the cages and locks
  + Protection: deter, delay, access
  + Justification: By ensuring that the cages are constructed properly and with locks, you can make sure that unauthorized people attempting to access these cages cannot simply break in.
* Fire sprinkler
  + Vulnerability: Water can damage the electronics
  + Security Control: replace water with chemical retardant
  + Protection: recovery
  + Justification: by replacing water-based fire systems with a chemical retardant that is safe for electronics, you will prevent damage to the data center in the case of a fire.
* Power generator
  + Vulnerability: Risk of tampering by malicious actors
  + Security Control: Protection barriers and access locks
  + Protection: deter, access, recovery
  + Justification: In the event of a black out, you want to make sure that the backup generator is working, and as such it needs to be secured against potential tampering.
* Fuel storage
  + Vulnerability: Flammable materials that can cause damage to people and property
  + Security Control: store the fuel offsite in a dedicated storage location
  + Protection: recovery
  + Justification: By storing the fuel away from the building, you minimize the risks that the fuel poses if a fire should break out.
* HVAC
  + Vulnerability: Cooled vents can cause condensation of moisture in the air
  + Security Control: Place vents in front of or below servers, not above
  + Protection: recovery
  + Justification: By placing the vents not above the servers, you will mitigate the risk of condensation of moisture damaging the servers.
* CCTV surveillance
  + Vulnerability: Wrong types of cameras will be ineffective for surveillance
  + Security Control: Ensure that the right type of camera, lens, lighting, and other considerations are kept in mind when installing cameras in different parts of the building.
  + Protection: detect, response
  + Justification: By ensuring the right types of cameras are used correctly, you can ensure the cameras are doing their jobs of detecting potential security risks so that security can respond timely and appropriately.

# Example

Roadway to the building

* Vulnerability: vehicle with malicious intent can approach the building at high speed and cause damage to building entrance
* Security Control: high curbs and speed bump installed on the approach roadway
* Protection: deter, delay
* Justification: slow down any approaching vehicle with speed bump and prevent vehicle from approaching building via off-road access