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.

Data center parking lot

* Vulnerability: any suspicious vehicle can park at the center and could damage the building with bomb
* Security Control: 20 meter perimeter monitoring the area, security guards and CCTV cameras
* Protection: deter, detect, access, response
* Justification: if the area is monitored it can ensure routine of which cars are familiar and any cars that are random or out of the blue as well as people that walk from the park lot to the data center

Building front door

* Vulnerability: unauthorized personal may enter and cause damage
* Security Control: specific security locks, monitoring
* Protection: patrol, deter, delay, detect, access
* Justification: prevent these people from going into the building, time is also bought through complex secure locks (and camera’s may pick up on suspicious activity)

Front lobby

* Vulnerability: social engineering, posing as someone else, taking advantage or manipulating receptionist/greeter, open area
* Security Control: receptionists and greeters should be trained to look out for personal who may be unauthorized and to ask them questions and have valid proof of the identity
* Protection: detect, access, response
* Justification: someone’s cover may break, or they may get caught and identified through subtle interrogation

Entrance into data center area

* Vulnerability: if entrance is not secure enough, someone who shouldn’t be there may enter
* Security Control: signs that display that only authorized personal should go in and it is monitored, cameras (depending on secrecy), and a secure lock
* Protection: delay, detect, access
* Justification: if there is a fear that they are being watched and the area is heavily guarded, some person is less likely to try to get in

Server cages

* Vulnerability: because they may have valuable sets of information, these are a target for accessing without permission
* Security Control: a lock that may perform an action (such as sound or no more attempts after a certain number)
* Protection: delay, detect, access
* Justification: after trying to access, this individual(s) will be afraid if there is something to scare them away

Fire sprinkler

* Vulnerability: although this is a safety measure, it can be misused as a sort of distraction or may also water damage if it is kept over a technological item
* Security Control: a protective cage around it that only opens when it senses fire and is alarmed for misuse, and technology is kept separate and away from them
* Protection: response, recovery
* Justification: it is important not to have it misused as it is there for safety and keeping it away from technology prevents information loss

Power generator

* Vulnerability: if not handled properly may be a safety hazard and hurt individual (electrocute them, burn, etc) and if there is too much power
* Security Control: keep a cage around them and the controls/switches, have a threshold of power that it does not cross and alerts the professional of danger or overpower
* Protection: deter, detect, recovery
* Justification: this ensures that only authorized people can access it with the necessary knowledge and skill set to handle it and a disaster does not occur

Fuel storage

* Vulnerability: stealing of resource for other means, not enough present or running out (as fuel is the blood of many machines)
* Security Control: keep it monitored, the amount and how much is being used and allocated and for what (keeping track and record)
* Protection: detect, access
* Justification: if there is a shortage, you can try why and where it went to and if not then perform an investigation to see if these is misuse occurring

HVAC

* Vulnerability: heating, ventilation, and air conditioning could be set to dangerously high or low temperatures which could affect comfort and even health
* Security Control: making sure there is regular checkup on the thermostat and recording devices that it is at a reasonable and realistic temperature according to external conditions (or at least at an average room temperature)
* Protection: detect, response, recovery
* Justification: making sure the temperature is reasonable and realistic ensures safety isn’t compromised of individuals

CCTV surveillance

* Vulnerability: misuse, using the surveillance for an ulterior motive or out of context, breakdown or technical difficulties of the cameras when they are required, not placed in a proper place where it is required
* Security Control: make sure they are monitored over important locations that are more vulnerable, like where confidential information and data is kept or resources that can be taken advantage of. Make sure they are working always and not just anyone can access them or muck around with them
* Protection: detect, deter (signage of them), response
* Justification: these cameras capture crucial information that may be required for an investigation and capture daily occurrences and keep track of the happenings in, around, and outside of the building and its premises