# Prevention: Physical Defenses




It's easy to only focus on cybersecurity controls, but if an attacker can get physical access to a system, it's usually game over. They can plug in malicious USBs, steal components such as hard drives, or damage systems so they can't be used. While this is not typically the responsibility of a cybersecurity team, it is definitely worth covering.

## DETERRENTS

**Security controls that act as deterrents include warning signs and barbed wire. Their purpose is to deter potential attackers and make them less likely to attempt to gain entry.**

- **Warning Signs:** Signs such as "DO NOT ENTER" and "You Are Trespassing" can be enough to make people turn around, as they have been informed that any further activity may be illegal.
- **Fences:** Chain-link metal fences are very common, with barbed or razor wire on top. This creates a barrier that can't easily be climbed over and requires more effort for attackers to bypass, slowing them down and giving more time for them to be detected.
- **Guard Dogs:** Security dogs that are trained to bark and cause distress are a strong deterrent. Despite being highly trained, they still appear to be dangerous in the eyes of the attacker. They are also able to help detain any intruders by holding them down until physical security personnel can apprehend the suspect.
- **Security Guards:** Physical security staff can act as a strong deterrent, showing there is a human presence on the site, and that if intruders try to gain access, it is likely will they get caught. This deterrent is enhanced on sites where armed security personnel are present.
- **Security Lighting:** Lighting is used to prevent low visibility areas caused by darkness, which could allow an intruder to bypass security controls such as CCTV and Security Guards. Lighting the areas in conjunction with cameras is a great deterrent and monitoring.

## ACCESS CONTROLS

**Access controls are used to prevent unauthorized people from accessing specific areas of a building or area.**

- **Mantraps:** These are a slow but effective security control, where an individual wanting to access a protected area must go through an initial door into a small holding room, where they are inspected from a window or

camera before the second door is unlocked.

- **Turnstiles/Gates:** This efficient control is very common in office buildings and requires employees to tap their ID pass on a reader, which will unlock the gate and allow them to pass through.
- **Electronic Doors:** These secure doors should be used throughout the facility, to limit the areas that a person can access, based on their role. For example, it is highly unlikely that someone from Human Resources should have access to a Server room. Only allowing certain people in specific areas not only reduces the risk of malicious activity but can also help find the person accountable as the list of potential suspects is much shorter.
- **Security Guards:** Physical security staff is able to check IDs or manually allow employees to access certain areas of a site.

## MONITORING CONTROLS

**These controls, such as CCTV cameras and intrusion detection systems are implemented to provide real-time monitoring and give security personnel the ability to:**

- **CCTV:** Closed-circuit television allows monitoring from multiple interconnected cameras, giving security teams expanded visibility.
- **Security Guards:** It's all good to have these technical measures in place, but there needs to be a team that is trained in their use and maintenance so they can fully utilize the security controls and respond to incidents.
- **Intrusion Detection Systems:** These systems have several different triggers that can generate alerts or set off alarms, including thermal (heat) detection, sound detection, and movement detection.

## CONCLUSION

By employing all three types of physical controls, organizations can work to protect their buildings and places of work from physical intruders that seek to cause harm to information systems or other assets. If malicious actors know that the organization takes physical security seriously, it acts as a strong deterrent and can work to reduce the risk of physical intrusions.

Previous Topic
Mark Complete
Next Topic
Back to Lesson