SLOAN
SECURITY GROUP

Scan to view on the web

WHITEPAPER

# Data Center Physical Security: Best Practices Every Plan Should Have

WWW.SLOANSG.COM

# Data Center Physical Security: Best Practices Every Plan Should Have

Physical security best practices can keep Data Centers secure from the perimeter all the way to the server rooms.

## Introduction

Data Centers have become a primary target for threats, terrorism, and cyber-crime. Data Centers all over the world store one of the most critical assets on the planet, data. They store and transfer highly confidential information for the government, businesses, and the personal details we share online.

When we think about attacks on data, we initially think of cyber-attacks that take place through technology networks. However, the physical protection of these assets that store and transfer the data is equally important. In order to ensure data is as safe as possible, physical security measures need to be taken seriously and carefully planned out to reduce the threat of a physical breach which may include an attack with the intent to steal or destroy data.

There are several physical security best practices to consider when keeping a Data Center secure from the perimeter all the way to inside the server rooms where the data lives.

## Use Physical Security Design Best Practices

Physical Security Design best practices include the 5 Ds. Deter, detect, deny, delay, and defend. The 5 Ds principle works on the 'onion skin' theory, wherein by adding multiple layers of security, they will work together to reduce attempts of attacks, prevent site access, give you time to respond to a breach, and deny and defend if necessary.

The deterrence layer is the visible barriers including anti-climb, anti-cut fencing, high-security gates, surveillance cameras, signage, watch guards, and more. The detection layer is the alarm function of these perimeter solutions and can be enhanced with additional non-visible monitoring solutions like drone detection, buried sensors, embedded sensors, hidden cameras, radar, lidar, or other detection systems.

The layers of detection solutions extend from outside the fencing to clear inside the data center cabinets and cabling infrastructure with multiple forms of alarms and monitoring 24/7. Data Center Infrastructure Management (DCIM) software manages and remotely controls electronic door locks, monitors real-time video feeds, and displays real-time audit logs which also helps following requirements and regulations.


## Install Video Monitoring and Intrusion Detection

Video surveillance and monitoring are crucial data to any successful Data Center security plan. The general best practice is to store surveillance footage and entry logs for at least 3 months, maybe longer.

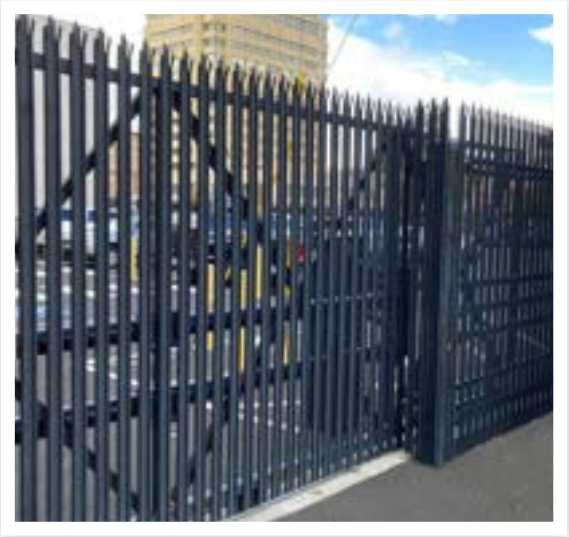
Detecting potential threats early on with the latest video surveillance can help security teams respond quickly to an unauthorized vehicle or person approaching the perimeter. Thermal camera technology with long detection ranges and higher-contrast images can track movement even in low-visibility conditions like darkness, fog, smoke, and light rain. Radar is another detection technology that can track movement in open areas and will be less sensitive to non-threatening activity from rodents, birds, and shadows which will reduce false alarms.

Data Centers can also benefit from implementing intelligent video with Video Content Analysis (VCA). VCA can be a powerful tool to quickly identify threats and identify license plates, faces, and other objects. Some of the most advanced VCAs can categorize objects using algorithms, machine intelligence, and smart technologies.

## Deny/Delay: Install Crash-Rated Perimeter Fencing and Barriers

Crash-rated fencing, walls, gates, bollards, and wedge barriers are critical to achieving data center physical security standards for the perimeter and vehicle access points. Data Center fencing should be built with steel pales or panels with anti-climb and anti-cut features. High-security gates should open and close quickly and satisfy similar anti-climb specifications and be crash-rated to withstand being struck by a vehicle. Crash-rated security cabling, beams, or bollards lining the perimeter may be useful to stop vehicles in areas where vehicles may be used to quickly breach a perimeter.

Choosing the right barrier products to fit the site design and surrounding environment can be challenging. Barriers are not always a “one-size fits all” scenario. Being open to using multiple barrier manufacturers will likely achieve the most effective perimeter protection outcome. Working with a physical security integrator is the best way to ensure the optimal product is installed and that those products work together with each other and to accomplish the 5 Ds principle (deter, detect, deny, delay, and defend).



## Create an Access Control Plan with Limited Entry Points

Data Center access control is critical, and it is vital to ensure that only authorized staff and vehicles have access to the area around the building and within the building itself. Creating a role-based access control system for staff and others can keep restricted areas to a limited group of individuals, making it easier to track access. It is also wise to have the fewest number of entry points possible into the Data Center perimeter and once inside. This will make it easier to monitor and manage those coming and going on a day-to-day basis.

An access control plan and procedure for vehicles to enter a Data Center is essential. Proper guard training, crash-rated gates, and barriers that occupy the entry lanes are some of the key ingredients to having a sound strategy.

Installing a wedge barrier, and crash arm/beam with an EFO (Emergency Fast Operation) option should serve as a final denial tactic.

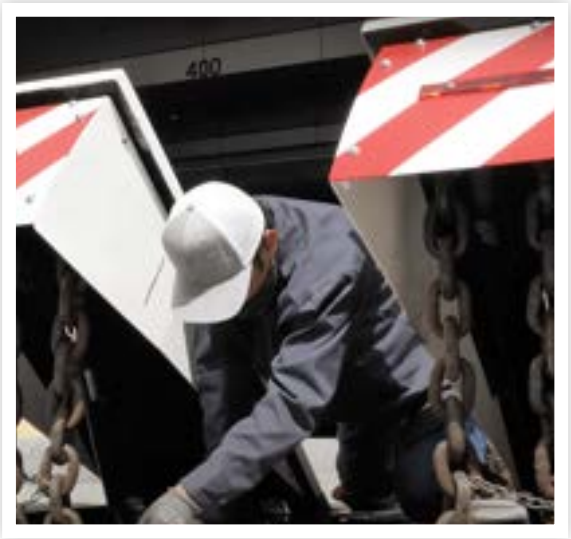
Data Center security teams should also be mindful of protecting guards positioned at the entry points into the Data Center, preparing them for worst-case scenarios. Installing a blast-resistant or bullet-resistant Guard Booth at the entry points will give the guards shelter if a violent attack is carried out.

## Defend: Implement Incident Management and Guard Training

Data Centers should have an incident management process with detailed documentation. It is a best practice to have a data center physical security checklist to ensure that all tasks are completed and accomplished in the correct sequence.

Performing threat response drills and security audits will keep personnel prepared in the event an incident occurs. During an incident, it is almost certain that stress levels and adrenaline will rise. Preparation is vital to performing under pressure situations.

Proper equipment training is often undervalued by Data Center managers. All who operate and manage the equipment should have adequate knowledge of how to operate barriers, when to run test cycles and who to contact when a repair is needed. Partnering with a company like Sloan can train personnel on their barriers, gates, and security components can help reduce human error and equipment malfunction.



## Perform Preventative Maintenance

Preventative Maintenance can improve the reliability and longevity of equipment like pop-up barriers, bollards, and automatic gates. Data Center teams can benefit from regular maintenance with improved performance and operational efficiency.

By working with an outside technical security services company for maintenance, Data Centers will have the support needed for success.

Finding an outside security maintenance company to work with will help keep equipment up and running and not require lost time from the Data Center's internal team with issues arise. Companies like Sloan Security Group offer 24/7 support for emergency repairs which is the best way to limit any unnecessary downtime.

## Conclusion

Data Centers are becoming more important than ever and attempted attacks are on the rise. Having a robust and comprehensive physical security plan is critical to keeping the data and people safe. As Data Center threats continue to grow, having a trusted partner to assist in your plan like Sloan Security Group is the best way to be prepared for the future. Being proactive and implementing some of these best practices will help Data Centers have a more successful physical security outcome.

If you have questions about Data Center Physical Security or need design assistance, please contact us.

SLOAN
SECURITY GROUP

## Contact

Sloan Security Group, Inc.
6828 W. Melrose St.
Boise, ID 83709
+1-888-382-8379

**WWW.SLOANSG.COM**