Guidepost

UNLOCKED: INTRODUCTION TO DATA CENTER SECURITY DESIGN

While principles of physical security are largely universal, data centers require a nuanced approach and are a great case study for security practitioners. In this blog, I will discuss basic security design for data centers and the new technologies now available to address the COVID era.

Looking ahead at commercial and industrial demands for data consumption, it is clear the data center industry will continue to thrive. Estimates on market growth average 15% year over year from 2020-2023. Whether you are evaluating your company's need to move data off-site or an owner investing in constructing a new data center for leasing, it is critical to understand the minimum physical security requirements. While your IT infrastructure is a given necessity, neglecting physical security can cost you and your clients time, money, and your company's public image.

Physical security always has the objectives to deter, detect and defend. A well-designed approach applies layers to the property where the innermost layer contains your most secure assets. Within data centers, the secure assets are either the owners' or their clients' business systems and data.

Consider the Location to Start the Design Process

A key element that should be part of any data center security design is the location and site selection. While there is a list of determining factors, one critical factor to note is CPTED, or Crime Prevention Through Environmental Design. CPTED is a holistic approach to design security into the built environment and make it more resilient and unattractive for incivilities, crime, violence, and terror. CPTED is based upon the concept that proper design and effective use of the built environment, can lead to a reduction in both the incidence and fear of crime (predatory stranger to stranger crime, and terrorism), while improving the quality of life (where we live, work, and play).

Is this an industrial/commercial site or a setting that is part of a residential area or downtown environment? Single buildings or multi-level buildings have other conditions that will need to be addressed.

While I am mainly focusing on the design and security within the data center these other areas are key in a master security design plan that affects the operations and security design within a given facility.

Reduce Risk with a Layered Security Design Approach

A layered security design approach requiring a progressively higher level of both physical and electronic security measures to move from a lower level to a higher level of security will significantly reduce risk and ensure only authorized personnel have access in and out of protected areas. Access control, video surveillance, intrusion alarm and duress systems can monitor, restrict, authorize, detect, and report events and unauthorized activities both in and outside of these facilities.

- The **first layer** of protective measures is the properties edge or property line. The goal of perimeter security is to clearly communicate the premise is private property and not open to the public. Typically, this includes a physical barrier, such as fencing and noticeable signage.

This initial layer of security also includes traffic flow controls (vehicular, personnel). Pedestrians should not be able to walk onto the property without running into barriers or authorized personnel. Impact-rated gates are the preferred choice to defend against vehicular attacks.

The size of your campus will determine whether security personnel also need to be present. Generally, larger campuses with multiple buildings could invest in security officers to be posted at strategic gate entrances – limiting access to only portions of a campus. Access control, video surveillance and intercoms are used to access, monitor, and communicate to the perimeter entry points accessing the property.

- The **next layer** of security covers the surrounding area of the building(s) setbacks. Parking lots are a common vulnerability point. Deterrence can be defined as creating a secure environment where negative activity is strongly discouraged. In open areas, a secure environment is curated by video surveillance, proper and adequate lighting, remote intercom assistance stations and noticeable signage. There could be physical separations from employee and visitor parking that require additional access control video surveillance and intercoms to move from the parking area to the building's access.
- The **third layer** encompasses access into the facility's visitor lobby. Some sites offer a more open sense or feel and the entry into the visitor/employee lobby is open during business hours. Others secure this entry by access control and the use of video cameras and intercoms to communicate and view personnel from within the building.
- The **next layer** involves a multi-authentication process that can consist of card read, PIN, and/or a biometric validation process. The most common include fingerprint, hand geometry and retinal scanning devices. These readers are set up to allow access through secure portals or mantraps that limit only a single person to access from the lobby into the secured corridor. The portals have anti-tailgating systems that monitor for a single authorized person passage through a portal. When the system detects more than one person trying to pass through the portal (piggyback) the system will generate an alarm and the portal door will remain secured. The operation of these secure portals is two-way, meaning you are required to present authorized credentials going in and back out. While generally only an authorized card read is needed, anti-pass back features can be implemented for higher security levels to track an individual's current location and movements throughout the facility.

Traditionally the lobby is where the security or visitor check-in and processing happens and the control or monitoring center are located. As with most secured facilities, all those entering the location will be speaking to security staff through ballistic rated panels and passing their ID and paperwork through a secured draw.

Once visitors and employees pass security and access the portals they are now in a secured corridor or a secured elevator lobby for multi-level sites. Again, valid credentials to access the door or call the elevator to access other floors will be required.

At this point you will need access control to enter the majority of any other locations within the building on a need to only basis and limited in duration (storage, electrical, mechanical, galleries, receiving/loading dock and offices). Most of these spaces will have video cameras positioned and recording activities.

- The **final layer** of security and the highest level is the data vault. This is where the rows of racks, servers and data storage are housed. At this level, multi-state authentication is generally required. However, this space if leased to a client may have additional security requirements to access such as:
    - Anti-tailgating devices or additional biometric devices specific to the client.
    - Card in and out with local alarms if card use is neglected leaving this space and anti-pass back features are enabled.
    - Access control measures deployed on specific racks limiting the number of authorized personnel.
    - Cameras to record entry points, as well as viewing specific racks, rack rows or entire camera coverage within the space.
    - Audit tracking from access control to video recording activities in the vaults is vital to the owner and their clients.

Securing facilities and limiting only authorized personnel is a must to limit the risk of business disruption, data breaches and public image. A layered security design approach can mitigate risk. However, the best physical security measures will fail if an organization does not provide and continually develop and enforce their policies, procedures, and staff training.

Since the COVID-19 pandemic clients are looking at new technologies and design concepts to protect their staff and clients by reducing or eliminating readers that require touching a device. This is the case when dual authentication is required from card and keypad (PIN) readers and some biometric devices. Iris readers and facial recognition cameras now can include thermal imaging to detect elevated body temperatures. These devices can also restrict access due to an elevated body temperature and alert personnel or deny access when face coverings are not worn. Scanning reader technologies such as the Morpho Wave readers can read hand biometrics without the need to touch the device. The hand simply passes across the scanners.

Other design changes include the increased use of auto door operators that are activated upon valid access from the access control system. When used on high activity doors this greatly limits the need to touch door handles or panic hardware to access and exit through doors.

These new technologies and design changes come at a price but are protecting owners, clients, staff, vendors and reducing risk that could impact the operations of a data center.

JON JOLIBOIS CSPM, PSP

Principal Consultant

With 36 years of experience in the security and low voltage industry, Jon Jolibois's in-depth background served as an embedded security consultant for Microsoft's data centers provides exceptional value to clients. He applies his knowledge with systems design and programming, site surveys, drawings and specifications, commissioning, and access control to ensure the integration of industry standards in an efficient and collaborative manner.