data center security

BUILDING A SOUND SECURITY STRATEGY

by Justin Hoffman

introduction

Data Centers, regardless of size and complexity, follow the same general guidelines for design and construction. Types of data centers include: Managed, Colocation, Micro, Enterprise, Cloud, Edge, and Hyperscale. Each type has a specific place and application in the world of data centers. A brief definition of each "type" is outlined in our Data Centers, Planning and Design white paper. A copy is available upon request.

These facilities face many security challenges and require robust protocols to mitigate against operational shutdowns, unauthorized access, and data breeches. Security measures are of paramount importance in design, construction and building operations.

growth

Facilities can range in size from an IT closet using 10kW of power to campus scale installations over 1 gigawatt representing billions of dollars of expense.

As Artificial Intelligence (AI) technology accelerates, the demand for data center capacity is increasing exponentially. Training large models requires significant computational power, particularly from Graphics Processing Units (GPUs). GPUs have become the processing powerhouse for AI applications like deep learning. Newer generations of these chips are demanding higher energy consumption and more advanced cooling solutions.

strategies

An important element of Data Center growth is the requirement for site, building, redundancy, and security. Data Center security is critical in the design and construction process and often includes multiple layers.

Overall physical security is a key consideration for data center design and protection. Improvement in cybersecurity, while critical, does not alleviate the threat of a physical breach that can render digital defenses useless. Design and construction of data centers must implement layered security measures that deter, detect, and respond to unauthorized access. Site and building access should be tightly controlled as outlined in the following security strategies:

SITE SELECTION

When selecting a site, significant attention should be given to those that mitigate the risk of natural & man-made hazards (unstable soils, flooding, earthquakes, hurricanes), crime rate, civil/political unrest, existing underground infrastructure, etc. Key planning metrics (**Zoning, Site, Infrastructure, Hazards, Power, Cooling, Connectivity, Emergency Response Time, and Speed to Market**) must be addressed in preparation for design and construction.

SITE PERIMETER

The data center and site circulation areas should be surrounded with a robust 8'-0" high metal fence. The industry standard for many years has been the Ameristar Impasse II Gauntlet Anti-Scale product.

As data centers have become more common, many cities require fence selection with a more "friendly" appearance. The Cochrane ClearVu is a good option while still providing protection from intrusion. Some municipalities have design standards that incorporate masonry piers or other decorative elements.

Certain users have requirements to prevent intrusion from vehicles. This can be accomplished with anti-vehicle ditches, berms, impact rated fences, cable barriers, rails, bollards, etc. Depending on the user, the site entry point will feature a security checkpoint with either a staffed booth to check visitor credentials or a pedestal with an intercom & key card reader. A combination of rolling or cantilever gate, barrier arm, wedge barrier, or tire shredder can be used to prevent entry by unauthorized vehicles. Two sets of gates/barriers can be provided with an operational sequence set in a sallyport configuration to avoid multiple cars entering. This is known as "piggybacking."

Entry points to data center campuses should feature a guard booth with separate entry lanes for visitors and employees. A separate entry lane should be provided for large trucks. Deliveries should be inspected via scales, sensors, and a visual check. A rejection turn-around lane should be incorporated for unauthorized visitors to exit without having to reverse. Adequate distance should be given between the public road and the guard booth to prevent the queue of entering cars/trucks from blocking traffic.

Parking can be provided outside the security perimeter where visitors leave their vehicles and are met by employees. Swinging man gates or turnstiles should be provided for foot traffic and as means of exiting to the public way in the event of an emergency. The perimeter fence can also be secured by video cameras with thermal and/or infrared function that provide automated alerts given when for movement is detected.

Plantings higher than 6-10" should be avoided within 6' of the fence line to avoid false detections. Ground sensors can detect vibration above & below ground. Visitors or contractors need to be on a pre-approved list for the day of their meeting for entry. Owner/operator will often require visitors to undergo background check before being allowed on-site.

BUILDING PERIMETER

The use of precast or tilt-up concrete provides economy and strength (or the appearance of strength) against intrusion. Glass curtainwalls and/or punched openings are often provided at the office or building's entry point. Glass walls should be protected from vehicles by impact-rated bollards, and anti-vandal film should be applied on the interior to prevent breakage.

Security cameras should be located on the building parapets with clear line of sight to the face of building with no blind spots. No plantings above 6-10" high should be located within 10' of building face.

It is preferable to have interior access to the building roof, no exterior stairs, or ladders for someone to gain unauthorized access to the roof. All exterior doors should be hollow metal construction with access control hardware. If an exterior door is for emergency egress only do not provide a handle on the exterior side. The building, generator yard, and surrounding area should be well-lit at night.

ACCESS CONTROL

Access control is a fundamental aspect of data center security focused on who has access to the building, utilities yard, and sensitive areas. Access control strategies are as follows:

- Employee and public entry are through an entry lobby with a security office. The typical entry sequence requires sign-in at a security desk for visitors and badged entry for employees.
- The security office will feature full-height wall separation from the lobby, a window with intercom, and a tray or transaction drawer. The walls and window may be ballistic rated. Guests are typically issued a visitor's badge and are escorted at all times.
- Depending on the owner, the lobby area may be sparse with only a few waiting seats or may include a refreshment area, conference room, restroom, etc. To gain access to the data center employees and visitors pass through a vestibule with two sets of doors, a turnstile, or circle lock (Boon Edam) with badge readers and occupancy sensors that prevent piggybacking.

BUILDING INTERIOR

Critical spaces (data halls, mechanical/electrical rooms, network rooms) and equipment storage rooms should be secured with access control hardware, such as card readers and/or biometric readers. Visitor and employee badges are coded and grant permission to certain spaces. Customer cages within the data center should also have additional card reader access.

UTILITIES

Similar to the building, critical on site equipment should be secured against unauthorized access. This includes the backup generator yard, fuel storage tanks, electrical substations housing transformers, switchgear, and batteries, etc.

Manholes for underground electrical or fiber optic connections should be locked and monitored. monitored.

CYBER

Key strategies include data encryption, firewalls, access control, and cyber hardening. Cyber hardening can prevent malware and other cyber threats from impacting access to sensitive data and interruption of operations.

REDUNDANCY

The reliability of data center operations and security systems is dependent on resilient power and infrastructure. As the growth in AI and high-density computing drive energy consumption, data centers must incorporate backup power systems, such as uninterruptible power supplies and generators that are capable of supporting critical operations and security functions during outages.

Redundancy should address all aspects of the infrastructure including power, network support, and cooling systems to prevent single points of failure. Regular testing of disaster recovery and business continuity is essential to ensure that operations can continue uninterrupted in the event of a crisis.

The capability for continued operations in the event of utility disruption is an important systems security consideration. The level of security and systems redundancy is dependent on the critical nature of facility data and operations.

Data Center redundancy is categorized in "Tiers" as defined by the TIA-569 standard. Each "Tier" is based on the requirements for redundancy, uptime, and cost. N = number of components or systems required for the full operation of critical equipment. Each of the four "Tiers" (I, II, III, IV) provide an increased level of system redundancy. A brief definition of each "Tier" is outlined in our **Data Centers, Planning and Design** white paper. A copy is available upon request.

summary

Data center security strategies should be embedded in the planning, design, and construction processes. Understanding system operations, space strategies, and future growth are key to implementing an appropriate security strategy.

about the author:

justin hoffman
AIA

Justin has extensive experience working with clients for master planning and design of data centers. Projects range in size from 100,000 sf to 360,000 sf and include managed, colocation, & enterprise centers with differing levels of operational redundancy.

point of contact:

steve kimball
PMP, LEED AP

Steve has over 40 years' experience with business leadership and project management. Prior to co-founding emersion DESIGN, he was the President and CEO for a 100-person A/E firm with offices in Ohio and Florida.

steve.kimball@
emersiondesign.com