# Holistic Data Center Security Design

## Six strategies to mitigate risks and maximize resilience

By Ryan Searles and Russ Hoppel

More than ever before, security and resiliency are vital components for ensuring uninterrupted operations of data centers, a rapidly expanding market that is expected to grow by 14 percent annually through 2030. Every new facility's computational processes, structural and operational systems, grounds, and staff must be protected against cyber-attacks, intruders, active shooters, natural disasters, and power failures.

Individual system redundancy, operational strategies, and safety policies go a long way toward mitigating threats and vulnerabilities. However, the most effective approach for maximizing the overall resiliency of today's and tomorrow's complex data centers is best achieved through integrated holistic security design.

Such an approach blends security strategies with technology, leverages AI-driven analytics, and integrates with resilient architectural and engineering design. It evaluates everything from cyber-security to the layout of hallways, exterior sight lines, fencing or vegetation at the perimeter of a property, as well as security cameras, access control systems, visitor management, and more.

**Safety** is the perception of how safe a person feels in their environment. **Security** refers to the various layers of tactical implementation used to achieve the desired safety. **Holistic security design** accomplishes both.

All types of data centers can benefit from holistic security, which is best accomplished when security is considered early in a new project's timeline. Accounting for the largest share of new data centers being planned today are high-compute facilities capable of processing energy-intensive artificial intelligence. While driving the rapid growth of the market, these facilities must overcome a host of obstacles standing in the way of achieving exceptional security design.

According to "Securing Data Centers," a report by the Security Industry Association (SIA), these obstacles include outdated specifications, siloed security systems, and speed-to-market pressures drawing in a wave of "partners experienced in other markets yet unfamiliar with the unique demands of data centers—all of which threaten the resilience of critical digital infrastructure."

This guide outlines six critical strategies for achieving holistic security of high-compute and other data centers, their physical assets, processes, and people.

## Strategy #1: **Include security early in design**

Including security during the design phase provides the most effective and cost-efficient solutions for mitigating emergency events, avoiding the potential loss of life, and providing an overall robust security program. Therefore, owners should have a security consultant on the design team from the very beginning. This allows collaboration with the architect and engineer, enabling all potential threats to people and assets to be addressed within a cohesive design that provides a high level of security that operates in concert with operational systems and other infrastructure.

Discussing security considerations from the beginning of design also provides savings for clients by avoiding change orders for adding security measures later in design or construction—costly endeavors that also may not be effective. For example, security cameras or other technology tacked on at the end of design may not significantly contribute to the building's safety.

In addition to including your security consultant early, make sure he or she is well-versed in the modern and specific needs of your new facility. For while many security strategies can apply to a variety of building and market types, not all are effectively transferable to data centers. According to the SIA, data center security specifications historically have been "frequently recycled from other industries or from older generations of data centers." This can result in failures including cameras mounted too high to perform facial recognition, license plate recognition specified at optically impossible angles, and access control readers that require multi-tenant sites to use "reader farms" because they cannot interoperate.

With a data-center-experienced design team that includes a security consultant brought on early, owners have taken the first step toward achieving holistic, integrated, and up-to-date security for their facility and campus in the most economic and effective manner.


## Strategy #2: **Create a security master plan**

Creating a comprehensive data center master security plan early in the planning stage is the best way to ensure that the desired outcome can be accomplished within an owner's timeline and budget. At the same time, the architect, engineers, and security consultant should work together to conceptualize and meet the owner's overall intent for their data center while integrating their respective systems.

The master plan should be driven by all characteristics and needs of the data center, including:

- **Type and ownership.** A federal-owned data center will have different security needs and requirements compared to a private, public, or multi-tenant/colocation data center. Likewise, the type and level of computational processing (e.g., high-compute vs. smaller, distributed edge data centers) also will drive security measures.

- **New construction versus re-use:** The need for speed-to-market is driving many owners to adapt existing urban buildings into data centers. The characteristics of such sites and structures will vastly impact the security approach.

- **Nearby infrastructure and site environment.** Proximity to other buildings, industrial or chemical plants, nearby highways, or busy roadways, etc., will inform security design—as will geographic factors such as the presence of trees that could obscure sight lines into or out of the building.

- **Distance from emergency responders.** Urban-based data centers generally are more vulnerable to man-made threats but are closer to emergency responders. Rural-located data centers, on the other hand, have less likelihood of such threats but still may need a high level of security given the fact that first responders will take longer to arrive in the event of an emergency.

Once all characteristics of a data center are documented and considered, specific security approaches and strategies, such as those that follow, can be applied to the master plan and resulting design.

## Strategy #3: **Crime Prevention Through Environmental Design**

A group of strategies, Crime Prevention Through Environmental Design, or CPTED, increases physical security without creating an overly institutionalized aesthetic by leveraging architectural and environmental elements. These strategies can include increasing natural surveillance, creating territorial boundaries, and establishing social management programs.

CPTED can be customized to meet any data center's unique characteristics and setting and can include any combination of the following:

- Vegetation and perimeter fencing, bollards, and gates to set territorial boundaries and direct visitor movement

- Open spaces for unobstructed sight lines to provide natural surveillance

- Open seating areas to encourage more watchful eyes in public spaces and deter crime

- Purposeful architectural elements that prevent loitering in public spaces

- Sufficient parking lot lighting

- Clear wayfinding throughout the property, both inside and outside

- Natural access control at the front entry

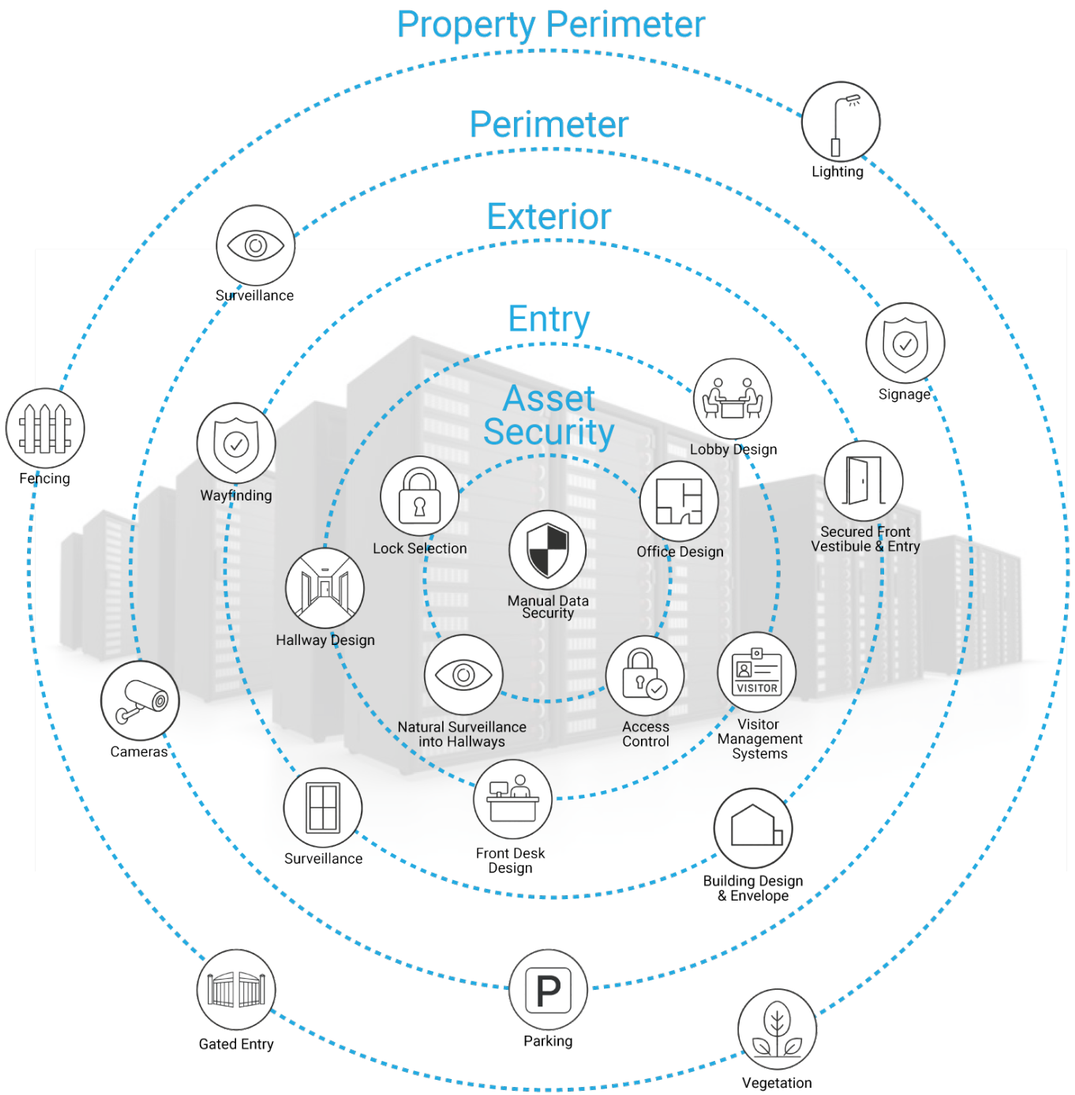
- Efficient use of security cameras

Designers and owners should work together to identify the CPTED options that work best for their specific project and create a plan to implement these solutions.

## Strategy #4: **: Concentric Circles of Design**

Another effective security design provides layers, or concentric circles of security. Each circle (see graphic at right) encompasses an aspect of security and technology, such as cameras, access control, building envelope, landscaping, CPTED principles, and more. All these circles work in tandem to provide an all-encompassing security plan.

As with CPTED, designers and owners should work together to identify the options within each circle that work best for their specific project and create a plan to implement the solutions.



## Strategy #5: **Technology and AI**

Owners need to look beyond simple bolt-on technology for their access control and security cameras and consider technology that supports all aspects and strategies of their facility's holistic security design.

Security technology has also migrated from hardware-based solutions to software-focused solutions, often as a component of an integrated intelligent building. Security-related technology will vary from building to building, but common state-of-the-art solutions for physical and cyber security include:

- Access control, including biometrics
- AI analytics for real-time threat detection, anomaly identification, and facial/object recognition in video surveillance with high-resolution cameras
- Quantum-safe cryptography to protect data from future quantum computing threats
- Smart locks and keyless entry integrated with mobile devices
- Visitor management

Owners also should test and validate their chosen technologies to confirm they will work as intended and that they integrate with other systems. Such verification should be done early in the project, well before any investment is made or construction begins. This provides risk avoidance as owners strive to deliver smarter environments by pushing the envelope with existing technologies and developing new ones when necessary. (For more information about technology validation and innovation, read about IMEG Labs.)

## Strategy #6: **Respond, Recover, Adapt**

Holistic security design also includes preparing your staff for the impact of an emergency event and how to respond afterward. The three actionable components of this strategy are to **prevent** or mitigate threats (as previously outlined), **respond** effectively in the event of an active threat, and **recover** post-event. Accomplishing the latter two components can be put in motion by:

- **Establishing a security champion.** Consider having a safety officer who is dedicated to the implementation and ongoing supervision of your data center's overall security strategies. This should also include regularly scheduled testing and verification of all technologies that support the strategies.
- **Enacting policy and procedures.** Develop a plan for your organization's response to threats, emergencies, and disasters—whether natural, technological, or man-made. The plan should include training employees to respond correctly and quickly in an emergency.
- **Establishing a chain of command** for senior management to respond quickly to an event and follow the company's specific procedures for reporting the incident, providing crisis management, and handling media inquiries. This will help your data center recover and remain operational during and after an event.
- **Remaining vigilant and up to date.** As those who perpetrate threats adapt their strategies to evade standard security measures, ensure that your tactics for preventing, responding to, and recovering from these threats also evolve.

Security design of your data center should be a thoughtful process that meets the specific needs of your facility, integrates with and supports architectural and operational systems, works in tandem with validated technology, and prepares staff to respond to a variety of events. This holistic approach will maximize the protection of your people, assets, and property, and help ensure your data center is resilient when a potential threat becomes reality.

*For more information, contact:*

**Ryan Searles**, CPP, CPD
National Leader/Project Executive
Security Design & Consulting Group
ryan.t.searles@imegcorp.com

**Russ Hoppel**
Senior Technology Designer
russ.c.hoppel@imegcorp.com

IMEG