The Security Challenges of Data Centers

securityinformed.com
Making The World A Safer Place

Johnson Controls
Security Products

About the author

An experienced journalist and longtime presence in the U.S. technology marketplace, Larry Anderson is the Editor of leading digital publications SecurityInformed.com and SourceSecurity.com. Mr. Anderson is the websites' eyes and ears in the fast-changing security sector, attending industry and corporate events, interviewing leaders and contributing original editorial content to the two sites. He leads a team of dedicated editorial and content professionals, guiding the editorial roadmap to ensure that SecurityInformed.com and SourceSecurity.com provide the most relevant content for industry professionals. From 1996 to 2008, Mr. Anderson was editor of Access Control & Security Systems magazine and its affiliated websites. He has written numerous articles for and about some of the largest companies in the security industry and has received numerous awards for editorial excellence. He earned a Bachelor of Arts in journalism from Georgia State University with a minor in marketing.

Content

This white paper was written in collaboration by
SecurityInformed.com and Johnson Controls

The Security Challenges of Data Centers

- By Larry Anderson

Data centers are a unique end user market with specific and distinctive needs when it comes to security. As the heart of the digital world, data centers are repositories of vast amounts of sensitive information, including financial data, personal information, and valuable intellectual property. Data centers also support critical infrastructure such as power grids, transportation systems and healthcare. In short, a compromised data center poses a threat to national security.

Protecting data centers obviously includes the most robust measures to avoid a cyberattack, but physical security is also top-of-mind. These buildings, containing rows and rows of servers that collectively make up the digital "cloud," must be protected from a variety of physical threats. The use of measures such as multi-factor authentication and biometrics reflects the highest levels of security. Protection starts at the perimeter and extends to all internal structures and each individual server.

This Technology Report, developed in cooperation with Johnson Controls Security Products, will focus on how physical security systems, including access control, serve the demanding environment of data centers. New data centers are growing at a double-digit rate in the foreseeable future. Therefore, developing the best physical security systems for these exacting environments presents a lucrative opportunity for the industry.

Data centers are vital to the digital world, storing sensitive information and supporting critical infrastructure, making their security essential. While cybersecurity is key, physical security measures like multi-factor authentication and biometrics are equally crucial to protect these facilities.

Data Centers Come in All Sizes and Types

When we discuss data centers, the term encompasses a variety of facilities and configurations. Some are enterprise data centers, which are owned and operated by a single organization to serve its internal needs. In some cases, a corporate data center might sublease some of its capacity to a neighboring institution, such as a nearby airport or state entity. Alternatively, there are "managed service data centers" operated by a third-party provider on behalf of a customer company.

At the higher end of the spectrum, there are massive data centers operated by tech giants such as Google, Amazon, and Microsoft. There are "colocation data centers" that allow outside companies to rent space, power, and network connectivity. A distributed network of data centers is used to deliver cloud services.

Given the variety of data centers, security requirements can vary. For example, a colocation data center might require more emphasis on perimeter security, while an enterprise data center might already be located inside a secured corporate campus. A colocation data center, given its variety of customer companies, might have more people coming and going, which would likely require more background checks, more credentialing, and extra effort to keep up with stringent protocols.

Variety of Data Centers:

Includes enterprise data centers, managed service data centers, massive tech giant-operated centers, and colocation data centers.

Colocation Data Centers:

Rent space, power, and connectivity to external companies, requiring stringent security protocols.

Enterprise Data Centers:

Owned by a single organization, sometimes subleasing capacity to nearby entities.

Data centers may seem to be a niche market, but it is getting bigger every day. Data centers are exacting and demanding customers, so expertise is paramount. "You really have to know what you're doing when you go into these environments," says Chris Bessert, Regional Sales Manager, Southeast, Johnson Controls Security Products and Software House. "You have to be cognizant of all the things happening around the data center, and why the data center infrastructure needs to be the way it is."

Data centers may seem to be a niche market, but it is getting bigger every day. Data centers are exacting and demanding customers, so expertise is paramount.

Security Requirements:

Vary based on the type of data center, with colocation centers needing more perimeter security and credentialing due to higher traffic.

Growth of Market:

Data centers are rapidly expanding, making specialized expertise critical for managing their complex security needs

Unique Solutions for Individual Applications

A variety of technologies are involved in securing a data center, from radar to cameras to various gates and barriers. There is no "typical" system for a data center – each customer is unique. Installing new systems starts with a discussion of the security needs of the specific facility. Customer discussions should include: What is your vision for this facility?

Typical elements include rack-mounted controllers, air-gapped systems, and use of on-premise software and servers. Other elements include the use of biometrics and multi-factor authentication, which increases security levels.

Discussions must encompass both hardware and software and include topics such as use of Lightweight Directory Access Protocol (LDAP), integrated video, mass notification, redundancy, and possible use of the cloud. "There is a whole slew of questions that need to be answered before you get into the specific security needs," says Bessert.

Given the high stakes of physical security in the data center environment, it is not surprising that top managers are often involved in the decision-making process. Because of the high level of interest in security, decision-making skews toward higher management. Those involved in security purchasing include members of the C-suite, the global director of security, and/or a dedicated security director. The chief security officer (CSO), director of information technology (IT), and hardware applications engineers are likely involved. Importantly, buying is a collective decision that is not made by any single person.

Diverse Security Technologies:

Data center security requires a tailored approach using various technologies, including biometrics and multi-factor authentication, with planning involving both hardware and software considerations. High-level management is typically involved in the collective decision-making process for security systems.

Multiple Layers of Security

The outermost layer of security is at the perimeter, where strong fencing systems, radar and video cameras are useful tools. Radar systems emit radio waves and analyze the reflected signals to detect and track objects. Video images may be validated using artificial intelligence (AI). Systems track who's coming and going. Guards are likely deployed to verify credentials, and there may be card reads, dual authentication, and/or facial scans. All these elements are deployed before anyone even gets into a facility.

Inside the building there are also various setups to track entrance of visitors and authorized personnel. Sliding doors may section off various areas and require validation to enter. Access control may be deployed throughout, including at the level of cabinets and racks, and there may be alarms to alert operators when a cabinet is opened.

Visitor management is typically deployed before a visitor arrives, via a web portal for example. When a visitor registers online, it triggers a vetting process to complete any required non-disclosure agreements (NDAs) or background checks and to generate any required documentation. When a data center invites a visitor, the system provides a credential such as a bar code or QR code that, in effect, says "I'm allowed to be here," for a specified amount of time.

Securing a data center requires layered protection, from perimeter defenses like fencing and AI-validated surveillance to strict internal access controls. To prevent insider threats, access is limited and activities are closely monitored, safeguarding sensitive information.

The Software House C▪Cure 9000 access control system from Johnson Controls includes a visitor management element to set clear and custom parameters around those individuals expected to access specific areas within a data center. The platform also can integrate with third-party visitor management systems. The system also integrates with other security elements, such as intrusion detection, glass break detection, smoke detection, door contacts, etc.

In addition to controlling the perimeter and access to a data center, there is another vulnerability to consider: Insider threats. Who could do nefarious things inside the data center, and how do you keep people honest? One of the ways to mitigate the possibility of an insider threat is to limit access to only one server cabinet at a time. Tracking how long someone spends in a specific area can also help to raise red flags. Given the importance of intellectual property stored in a data center, guarding against sabotage or theft is all the more important. Any information that gets outside the data center could destroy a company's reputation.

Access Control:

Internal access controls include sliding doors, multi-factor authentication, and alarms at the level of cabinets and racks.

Insider Threats:

Mitigating insider threats involves restricting access to specific server cabinets, monitoring time spent in areas, and tracking activities within the data center.

> *Platforms like the Software House C▪Cure 9000 integrate visitor management with intrusion detection, smoke detection, and other security elements.*

Challenges of Securing a Data Center

Challenges of data center security include the need to avoid wireless communication, to minimize system footprint so as not to compete for income-producing rack space, and to keep costs low.

Wireless connectivity, including WiFi, for example, cannot be implemented in data centers because the electronic “noise” it creates at 2.4 gigahertz can interfere with operation of computer servers. Also, security systems need to be completely separated (“air-gapped”) from the data center’s computer servers. Power-over-ethernet switches are mostly avoided. Wired connectivity also prevents uncertainty about possible cybersecurity vulnerabilities.

When keeping IT technology up to date in a data center, it is critical not to overlook the security system. Although it is separate from other systems, security is also an IT application, using servers. Keeping equipment and protocols updated ensures the system runs securely.

A systems integrator plays a significant role in securing a data center. Primarily, a systems integrator has a broad view of the entire system, not just a single element, whether video or access control. Manufacturers serving the data center market are most successful when they go into the project as a team alongside the systems integrator.

Avoidance of Wireless Communication:

Wireless technologies like WiFi are not used in data centers to prevent electronic interference and cybersecurity vulnerabilities.

Air-Gapped Security Systems:

Security systems need to be completely separated from the data center’s servers to ensure security and reliability.

Johnson Controls has a broad presence in the data center market, including a systems integration group, and across the fire, HVAC, and security markets. The company is well positioned to provide a combined package and a turnkey solution to meet a data center's security and broader technology needs.

On the equipment side, Johnson Controls provides access control and video surveillance systems and equipment through a multitude of dealers and integrators in the channel. For example, the Software House C•Cure 9000 access control system encompasses software, controllers, readers and other components that accommodate the varied needs of data centers. The JCI equipment divisions can collaborate with other divisions to build, lay out and deploy the right technologies. Alternatively, they also work with outside dealers and integrators on data center projects.

> *A systems integrator's broad view ensures seamless security across a data center's complex environment.*

Johnson Controls' Capabilities:

Johnson Controls provides a combined package of fire, HVAC, and security solutions, offering turnkey solutions tailored to data center needs.

Collaboration with Dealers and Integrators:

Johnson Controls works both internally and with external dealers and integrators to deploy customized security and technology solutions for data centers.

Deploying OSDP at the Lock Level

Access control systems in data centers that deploy Open Supervised Device Protocol (OSDP) are able to improve interoperability, ensure reliable two-way data exchange among devices, and provide other advanced features.

Open Supervised Device Protocol (OSDP) is an open standard protocol that utilizes highly reliable R485 protocol supporting 2-way high-end AES-128 encrypted communication between devices and controllers. Constantly monitored wiring through OSDP ensures higher reliability and security of communication in comparison to older protocols used in Wiegand communication.

Use of the OSDP protocol, instead of Wiegand or RS485 serial communication, adds more logic to the security of access control systems, expanding capabilities. OSDP is a communication protocol specifically designed for access control systems, developed to enhance security, interoperability, and flexibility compared to older protocols. OSDP allows for two-way communication between devices, which enables advanced features such as real-time status updates, device configuration, and troubleshooting. Also, using OSDP, firmware can be updated more easily, and everything is encrypted. Johnson Controls is rolling out OSDP as an option across the majority of its

Johnson Controls Integration:

OSDP is being rolled out across Johnson Controls' security products, enhancing security and reducing costs by improving functionality and minimizing infrastructure needs.

Assa Abloy KS210 Server Cabinet Lock:

Uses OSDP to secure more cabinet locks with fewer resources, decreasing rack space and infrastructure requirements while integrating with Software House C•Cure 9000.

entire security products line, achieving enhanced security, improved functionality, and lower costs.

One access control solution at the rack-mount cabinet level is the Assa Abloy KS210 Server Cabinet Lock. The lock integrates seamlessly with Software House C•Cure 9000 access control to protect assets from intrusion and expensive downtime. The KS210 lock is a 4-wire solution that uses OSDP, which decreases the infrastructure needs of protecting data center cabinets. Using OSDP, a system can empower 32 locks with the same infrastructure previously required for eight locks. Instead of running individual wires to lock components, an OSDP module in the reader uses two-way communication to "daisy-chain" a row of cabinet locks using one connection to the panel.

The approach delivers on the need of data centers to minimize costs and infrastructure (e.g., rack space). At the same time, it provides real-time visibility into what is happening at the most precise level of the data center, which is especially useful to detect and monitor the possibility of insider threats.

KS210 can secure the cabinets in large sections of a data center using a single controller, thus minimizing rack space, wall space, and general infrastructure. The ability to secure more doors with less cost and less infrastructure is huge for data centers, where rack space is at a premium and there are large operating costs. Using fewer controllers with any project can save thousands of dollars while securing the same number of locks. Rather than thinking about access control in the traditional way, a more flexible and scalable approach pays dividends in better security at less cost.

Using fewer panels also minimizes power costs, a perpetual concern for data centers hosting rows and rows of power-hungry servers.

OSDP provides advanced security with two-way encrypted communication and real-time status updates.

The Power and Promise of Scalability

Scalability is a useful element for security systems at data centers, which is also related to the need to minimize infrastructure. For example, if a controller can accommodate eight access control readers, what happens if a customer wants to add more readers? In one scenario, the expansion might require an additional controller (more infrastructure). Or it might require the replacement of an existing controller with one that can accommodate more readers.

Greater scalability can address this scenario more economically. In the case of Johnson Controls iSTAR access controllers, enhanced scalability enables the addition of modules to increase the capacity of an existing controller up to 32 readers. Scaling up also enables customers to embrace OSDP, biometrics and other enhancements more cost effectively. For example, adding locks to cabinet racks does not require additional controllers if the capacity of current controllers can be expanded.

Scalability in data center security systems enables expansion without extra infrastructure. Johnson Controls' iSTAR controllers can add up to 32 readers, allowing cost-effective upgrades like OSDP and biometrics integration.

Scalability is essential for minimizing

Scalability is essential for minimizing infrastructure while expanding security systems in data centers.

Implementing Brands and Services Holistically

“We strive to be good proponents of security, understanding that data centers are growing exponentially,” says Bessert. “Data centers are aware of the important role they play in the world, and we try to offer the best possible solutions for security, cost savings and energy savings. JCI has a fantastic breadth of brands and services that can be implemented in a holistic way in data centers.”

In the end, it’s all about the customer. “You really have to be a true consultant about their specific needs,” Bessert says. “No two data centers are the same and you must earn their trust. They are dealing with a lot of sensitive information. You must take that into consideration when you have those conversations. Be sure to do your due diligence and help them achieve their goals. I learn something new every time.”