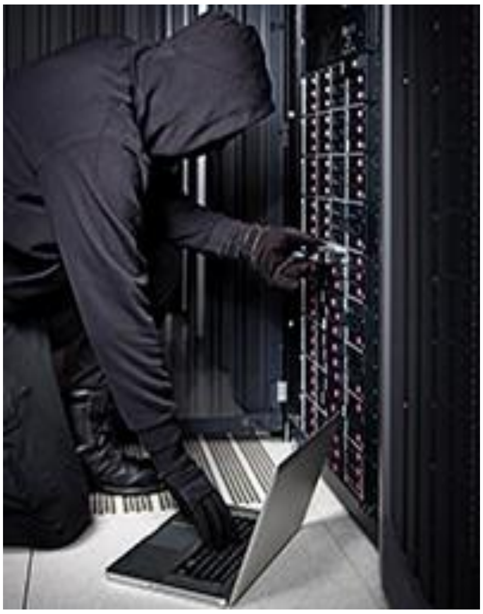
www.pipelinepub.com
Volume 19, Issue 9

Rethinking the Role of Physical Security in your Data Center IoT Network

By: Mark Feider



Physical security systems have always been critical to data centers. But now these systems—including surveillance cameras, video management systems (VMS), access control systems (ACS), automated license plate readers (ALPR), and intrusion systems—are connected to IT networks. As such, they can be a source of vulnerability for cyberattacks.

On the flip side, connected physical security devices collect a vast amount of information that data centers can use for valuable insights far beyond security. These systems are moving beyond being seen as simply a tool for risk mitigation. They can now be part of your data center's overall digital transformation.

Having a unified system with a strong cybersecurity posture helps ensure that your system is protected from cyberattacks, provides valuable insights, and streamlines compliance.

Closing up Cyber Vulnerabilities

There's a growing awareness of the cybersecurity of physical security systems. Outdated technology can leave data centers vulnerable to cyberattacks that exploit software vulnerabilities in connected systems. There's no difference in the result if a server room is breached physically or through a cyberattack on a surveillance camera, air-conditioning system, or laptop.

As cyber threats grow, physical security and IT must work together to safeguard network infrastructure. A unified IT and physical security team can develop a comprehensive security program based on a common understanding of risk, responsibilities, strategies, and practices.

As a first step, your team can conduct a *posture assessment* to identify devices of concern. This involves:

- Identifying their functions and confirming their role/relevance
- Maintaining information about each physical security device (connectivity, firmware version, and configuration)
- Documenting all users with knowledge of physical security devices and systems

Based on the findings, the team can recommend improvements for individual devices and the entire system. It's also important to implement a schedule of ongoing testing and reassessment of all inventoried devices to manage risk.

Cybersecurity best practices include:

- Implement end-to-end encryption to protect video streams and data in transit and storage
- Disable access methods that don't support adequate security protection
- Replace defaults with new passwords and change them regularly

As new cybersecurity updates are announced, update management can be improved by defining who is responsible for tracking, vetting, deploying, and documenting available updates. You can also enhance access defenses with a layered strategy that includes multifactor access authentication and defined user authorizations.

Speak with your systems integrator or manufacturer about more cybersecurity strategies. They can work with you on a plan to ensure you have a strong cybersecurity posture.

Tapping Physical Security Data to Improve Operations

Protecting customer data is the top priority for any data center. To achieve this, many have security personnel monitoring systems 24/7 to respond to incidents as quickly and effectively as possible. Unfortunately, working with isolated or siloed video management and access control systems can slow down response times. They require operators to move between applications to piece together important information.

Isolated systems also make it more difficult to automate alarms, leaving data centers to rely on security personnel to actively monitor inputs and identify specific security threats. But security teams can quickly become overwhelmed with the amount of information coming in. This can lead to increased system and data vulnerability as important information is lost, ignored, or overlooked.

Having sufficient data management and structure is key to unlocking the value of that data. Unifying physical security systems on an open platform can help.

The first step for using data for operational insights is *discovery*. Data analytics offer the best insights when they're deployed to confirm a hypothesis, rather than a solution in search of a problem. Identify the questions you're trying to answer. Are you looking to find out why the security team gets double the amount of "door open" alerts from the same three doors? Who's parking in unauthorized spaces at your data center? Which HVAC systems are working or offline? Once you've defined the questions, determine who needs to answer them, who has access to the data, and how it is accessed.

Applying the Data Available Through Your Physical Security Systems

A unified physical security platform can centralize both video analytics and data analytics to deliver a global view of your operations from a single interface. It can then be applied to automate and measure operational steps across a range of use cases:

Understanding anomalies

You can use data analytics to understand not only when breaches occur, but the circumstances and problems leading up to them. Run system health and monitoring reports to identify the most common anomalous events and explore them more deeply. If all your "door open" warnings are coming from the same three doors, for example, maybe those sensors need to be adjusted or the locks changed.

Verifying who is on site

Data from automatic license plate readers (ALPR) is often overlooked, but it can deliver a range of insights. It can provide information on which cars were in the parking lot when an incident occurred. This helps facilitate investigations or confirm which contractors or employees were on site at particular times and for how long.

Integrating data from other systems

When you bring data from many different sources into one place, you get a more complete picture of what's happening throughout your entire data center. A unified, open physical security platform can centralize data for better visibility, operations, and intelligence. Integrating data from systems that track facility data with security system information provides a richer context that can then be analyzed.

Streamlining compliance

Data centers can store and secure data for hundreds of companies from various industries all at the same time. This means that the centers must be able to comply with the standards set by each industry.

For example, a single data center could have to comply with the Health Insurance Portability and Accountability Act (HIPAA), the General Data Protection Regulation (GDPR), the ISO 27001 information security standard, and the Service Organization Control (SOC) and SOC2 standards. Complying with these standards requires consideration of how physical security systems are configured and managed. With modern security systems, processes can be automated to ensure compliance, provide faster situational awareness, and reduce the amount of labor for physical security guards and administrators.

Collaboration Between Security and IT Teams Is Key

Modern physical security systems are IP-based and network-connected. They present cyber vulnerabilities and data opportunities. Both are best addressed by strong collaboration between security and IT teams.

A unified, open physical security platform helps data centers tap the full potential of devices and equipment they already own. They can use operational insights in new ways and strengthen their cybersecurity posture across multiple systems. And it brings teams across the organization together on a common toolset, using a common language, to gain insights and improve the things they do every day.

Data centers must keep up with evolving regulations and security threats while ensuring that their customers' needs are always met. The right solution can bring together and centralize these considerations. It can reduce security risks, improve decision-making, and enhance compliance. Upgrading to a unified security platform provides a foundation that enables data centers to grow effectively and continue providing the services their customers want today and in the future.