BUILDINGS

SAFETY & SECURITY

Physical Security for Facility Managers: What You Need to Know Now

Now is the time to assess your physical security setup. New technologies can help you manage risk more effectively and improve business operations.

Mark Feider

Building safety and security requirements have been redefined in recent years and physical security systems need to keep up. They've evolved from handling video surveillance and access control to becoming key to an organization's digital transformation.

Now is a great time to assess your current physical security setup. It's likely that newer, more powerful technologies can help your organization manage risk more effectively while improving business operations.

Unify Functions on a Single Platform

The primary goal of a physical security system is to keep people, facilities and assets safe. These functions are often interdependent and work best when they are unified on a single platform. Unification gives users a consistent experience across security tasks. For example, a user could spot a door propped open, review video and determine why it was left open and by whom, and provide reporting and trend analysis by door or user over time, all from the same interface.

Unification is different from integration, even though the terms are often used interchangeably. Integration relies on connections between independent solutions from multiple vendors. This often includes a patchwork of APIs or interfaces that connect disparate systems. Managing integration points is costly, and too often the cost increases with time. Unification is more than integration. It brings all security applications together to address a broad range of security tasks, manage security policies, monitor events and run investigations. It's built from the ground up as a suite of products, using the same foundation to build, evolve and expand security operations over time.

More workloads are moving to the cloud, and it's important to find a truly

hybrid platform that lets you run workloads where it works best for your organization. Unification can include cloud and on-premises solutions, native and third-party data sources, and components from a variety of vendors. All these capabilities co-exist transparently, and scale seamlessly as new technologies are added.

Consider an Open-Architecture System

No one wants to be locked into old technology. An open-architecture system uses non-proprietary components that can be sourced from third parties, allowing organizations to add components and possibly reuse existing components as needs evolve. Video cameras, access control modules, intercoms or other equipment with an open architecture give organizations maximum flexibility as business needs change. Open architecture is also easier to maintain because of the availability of third-party parts and is often less costly.

Evaluate Cybersecurity Capabilities

Open architecture does not mean that systems are unprotected; they are just easier to scale and maintain over time. Cybersecurity remains a separate, high priority for any technology, including physical security systems.

Built-in cybersecurity tools make it easier to protect against possible threats, monitor system health, and stay resilient in the face of cyberattacks. Look for solutions that hold ISO 27001 certification or equivalent and include cybersecurity features by design such as encryption for data, servers, and all communications, and granular authorization processes.

Correlate Data for Better Outcomes

Modern physical security systems have a single dashboard that shows the full range of security and operational data. As data converges into a single

view, insights into trends and patterns emerge that enable quicker, better decisions that improve safety and operational efficiency.

Not all shared data is specific to a security incident. Sometimes organizations want to track generalized information about visitor, employee or vehicle activity to support visitor management, employee experiences and traffic flow. This type of aggregated data provides information about broader trends while maintaining individual privacy. Critical data insights inform a range of facility operations, such as parking space utilization, traffic patterns and building occupancy to create more convenient, efficient experiences.

While data from unified physical security systems can provide valuable insights, organizations must also protect data privacy. Regulations establish a minimum standard for how personal data should be stored and managed, but organizations can do more than the bare minimum. A modern security platform can include features to help you ensure that only authorized people access the data. Given accessibility management, it's possible to control and monitor video while preserving individuals' privacy by pixelating faces in videos to blur identities. Equally important is keeping detailed audit trails of all activities on the platform, including who accessed data and when.

Extend Usage for More Business Impact

Physical security systems operate successfully on their own to mitigate risk. When connected with building automation tools, they provide even greater protection and efficiencies for building operations. Security systems that collect data about building usage and occupancy can feed automated building systems, such as elevator dispatch, lighting, fire or HVAC operations to streamline processes or schedule optimal maintenance.

With the rapid proliferation of Internet of Things (IoT) technology, the uses will only grow. Managers can use data across their systems to support their

decision making. A physical security system's ability to connect seamlessly with intelligence tools is rapidly becoming an essential capability. This expansive view helps drive revenue and achieve efficiencies through smarter buildings.

Work with a Reliable Partner

While it may seem obvious, one of the most important decisions you can make is to choose a trusted technology partner to guide your organization. Look for a physical security vendor with a stable financial track record and technology expertise in your industry. It's always a good idea to check with other companies or peer groups for recommendations.

After identifying vendors, dig a little deeper into how they plan to invest in future technologies. What percentage of their budget do they invest in research and development? What is their timeline for continual product updates? Look for a partner with a smart business roadmap that will grow with your organization.

A forward-thinking collaboration with a physical security systems partner will be the most cost-effective way to stay current in the long run. The goal is to be able to keep your security systems up to speed by easily adding new technology and sensors as they become available. This ensures you can continually maximize value to your business. A vendor's approach to evolving technologies will be critical to their success—and yours.