BUILDINGS

ADVANCE TO TOPICS

ENSURING SAFETY & SECURITY FOR TODAY'S BUILDINGS: PRACTICAL GUIDANCE FOR OWNERS AND FACILITY MANAGERS

Contents

Introduction

Commercial building safety and security measures are of paramount importance for facility management professionals today. These safeguards serve as the first line of defense against a wide array of physical and cybersecurity threats that can disrupt operations, harm occupants and inflict significant financial and reputational damage on organizations that may impact a company's business continuity.

Physical security measures are designed to safeguard the physical infrastructure of a commercial building from various threats, including theft, vandalism, arson, and even acts of terrorism. In an increasingly digital world, cybersecurity is another significant facet of commercial building safety that cannot be ignored. Facility management professionals must consider the vulnerability of a building's technological infrastructure, including computer networks, data centers, and communication systems, to cyberattacks.

That's why we at *BUILDINGS* magazine have compiled this eHandbook on building safety and security to give building owners and facility management professionals practical guidance on how to address these threats to their building portfolios. In this digital resource, you'll find a variety of articles that address both physical and digital threats that put your buildings at risk with solutions you can put into practice today.

The role of facility executives in establishing and maintaining safety measures is indispensable in an ever-evolving landscape of security challenges and technological advancements. By proactively addressing these concerns, facility managers contribute to the overall success and resilience of their organizations. We hope this eHandbook will help in those efforts.

Sincerely,
Janelle Penny
Editor-in-Chief, *BUILDINGS*

FM, IT and Security: How to Break Down Silos for Better Outcomes

FM, IT and security have historically been siloed from each other. Break down those barriers and deliver better results together with these 6 tips.

By Janelle Penny

How closely do your facilities and security departments work with IT?

All three have historically operated in their own worlds, but the rise of connected buildings and smart technologies has made it critical for these departments to work together for the good of their organizations. FM, IT and security leaders who don't—or won't—reach out and work together with other teams are putting their organizations at risk.

Start by understanding where the silos come from—and then break them down to deliver better results together.

WHY ARE THESE DEPARTMENTS HISTORICALLY SILOED?

FM has always worked in the physical space, while IT has historically had domain over technology and virtual environments, explained Laurie Gilmer, immediate past chair of IFMA's Global Board and president/COO of Facility Engineering Associates, PC. When these two departments did interact, it might be because IT needed a server room to be cooler, for example.

ID 47303660 © Rawpixelimages | Dreamstime.com

Then, as integrated workplace management systems (IWMS) and computerized maintenance management systems (CMMS) began to grow in popularity and complexity, the two fields began to merge in ways they never had before.

"You saw those more centralized management systems for facility managers, and they needed to sit somewhere and be on perhaps a central server," Gilmer explained. "Some IT managers understood what the capabilities are and would work with FM. Others would treat it as 'That's not really my territory. I don't want that stuff on our servers. We'll put it on a special computer for you.'"

Security followed a similar path, evolving from a more physical solution into a more IT-centric solution over time, said John Joyce, director of sales, enterprise markets, for Genetec, a unified physical security provider. "More and more devices are on local area networks or wide area networks, and it's been a natural progression for physical security and IT to come together, work together and solve problems together," he explained.

It's tempting to think about IT as living in a digital universe that doesn't affect the physical world where FM and security operate. However, nothing could be further from the truth. Bad actors can infiltrate your building through any connected equipment and wreak havoc on your organization. Gilmer described a recent example from a security conference where a facilities person clicked on a photo that appeared to be from a colleague and inadvertently launched a massive attack. The perpetrator began burning out the VFDs on the motors in the central plant to extract a ransom.

"A central plant's job is to keep things cool or warm. Whether it's boilers, chillers or condensers, water needs to be flowing for the building to do what it needs to do," Gilmer said. "If you lose chilled water, you lose cooling not just for your thermal comfort systems, but also some of your critical systems, like your IT infrastructure. Most facilities have redundancy in pumps, but what they don't expect is for all the pumps to go out at once. You essentially start losing the building."

Examples like these are alarm bells underscoring the importance of cyber security and a good partnership between FM, IT and security. FMs don't have to be experts in these areas, but they do need to work together to anticipate risks and mitigate potential disasters. Finding a mutual understanding is a good place to start.

HOW TO BREAK DOWN THE WALLS

FM, IT and security are all different, but they have one common mission: keeping their organization up and running. Each of the three are essential players in accomplishing this mission. That's why it's so important for them to work together. Here's how you can start building a unified strategy.

1. Learn what the other departments do. This is not always easy because these departments famously have a lot on their plate but try to "understand what the other side cares about and what its job is and make that connection," urged Gilmer.

2. Spend time with other departments. If you're in the facilities department, go meet the IT and security people and see what their day looks like. What do they care about? What do they need? "When you spend time with someone, you can really begin managing the relationship and understanding one another better," Gilmer said.

3. Attend conferences. There are great cyber security conferences out there that could be instructive for facilities personnel. FM conferences like IFMA World Workplace can be useful for IT and security. The goal is to broaden your perspective in ways that will help you work smarter.

4. Partner for a threat analysis. Once you've started building or improving relationships, start taking concrete steps to harden your facility. Think about potential cyber threats. How likely are they? How could a bad actor gain access to your facility and what damage might they be able to do? Bring IT, security and FM together for tabletop exercises and use those as the basis to shore up your plans.

5. Look at replacement strategies for devices and systems. Some devices will represent a higher cyber security risk than others. "Strategies that promote modernization are going to be critically important," Joyce said. "Where we've moved away from these individual systems, we've got more unification and integration in place in facilities. That's helping that conversation along because we're no longer dealing with multiple types of systems. … It's a multifaceted effort based on the way the technology has evolved."

6. Keep communicating. Your job isn't done after you update your cyber security plans and have one tabletop exercise. Keeping your facility running in top shape requires you to maintain these relationships day in and day out.

"If you have one weak link in the chain, you are susceptible," Joyce said. "Communication between these groups, understanding what the other one does and how they maintain their equipment and devices, and an overreaching comprehensive strategy are critically important."

Added Gilmer, "Never stop learning. Never stop reaching out. Work to understand those things that are pretty soon going to be knocking at your doorstep if they aren't already."

Photo 127452233 © Funtap P | Dreamstime.com

Smart Buildings Require Smart Cybersecurity: 5 Tips for FMs

It's time to adopt a mindset of zero trust when it comes to cybersecurity. Harden your facility against attacks with these 5 protocols for facilities departments.

By Jennie Morton

Why are commercial facilities an appealing target for cyberattacks? While most businesses protect employee and financial data, they overlook a simple fact—every building system connected to the internet is at risk of being hacked. It's a massive opportunity for a bad actor to not only disrupt operations but endanger lives.

While cybersecurity practices may feel daunting, they're not a lost cause. Every precaution your organization implements fortifies the digital side of your building's footprint.

"Don't get overwhelmed—just start. Cybersecurity is a process you have to mature through," stressed Fred Gordy, director of OT risk assessment with Michael Baker International. "The goal is to be less vulnerable than you were yesterday."

WEAPONIZING COMMERCIAL BUILDINGS

Did you know that real estate is considered critical infrastructure by both the Department of Homeland Security and the Cybersecurity and Infrastructure Security Agency? One reason is that facilities are prime targets for a threat known as killware.

“Rather than a type of virus, killware attacks are meant to cause property damage, human harm and even deaths,” Gordy explained. “It doesn't take much either. Boilers can be turned into bombs, lights turned off so people fall down stairs and electrical panels shorted to start fires.”

“Most people can't imagine what could go wrong with a building if it were hacked. But if someone gets control of its operational systems, they can make it a dangerous place,” added Jim McGlone, CTO of Automation Strategy & Performance, Inc. “For example, there was an attempted attack in 2021 of a water treatment plant—the goal was to poison the water by altering chemical levels. Private and public buildings are just as vulnerable to being weaponized.”

How is this possible? First, many building systems are openly exposed on the internet with few security protections. IoT devices are a double-edged sword because everything is connected. By breaking through one point, the rest of the network is accessible.

Second, an interface or direct communication between building and corporate systems is a massive risk. A bad actor may not care about HVAC, but your mechanicals could be an attractive portal if they provide a connection to enterprise data.

The good news is that the principles of physical security—creating layers of barriers—is the same for cybersecurity. These safeguards will thwart someone from penetrating your systems and data. Lock down where building controls interact with your electronic perimeter.

“Because bad guys will troll your digital neighborhood, cybersecurity is no different than physically hardening your building to send the message ‘We're protected,’” Gordy stressed.

5 CYBERSECURITY PROTOCOLS FOR FM

There are entire books devoted to cybersecurity best practices. Your IT department should also be a robust partner in this effort. You can implement ISA/IEC 62443, a series of cybersecurity standards for automation and control systems. Follow the basics of changing passwords, be suspicious of links or attachments, perform weekly backups and control remote access.

But nothing will ever be accomplished without an attitude shift first. Cybersecurity begins as a mindset more than anything.

1) Implement Server Protocols

“Treat every computer that runs building controls like a server,” emphasized Gordy. “Don't use those devices for direct internet access either. They should be locked up as well.”

2) Check What's Exposed

“You'd be amazing at what's unprotected. How far does the Wi-Fi extend outside of your building? Do you have unused ethernet jacks that are still active? Who has access to your IT closet?” asked McGlone.

3) Update Your Device Inventory

“Know what you have, how it's connected and who has access. If you don't have an accurate network diagram, you can't keep the boundaries safe,” said Gordy.

4) Isolate Building Systems

“Create a DMZ network to isolate operational technology, which is a type of segmentation that only allows specific traffic with certain permissions,” McGlone recommended.

5) Screen Everyone

“Adopt a zero-trust policy, which means ‘Never trust, always verify,’” says McGlone. “This is critical for any visitors and vendors bringing their own device. Start screening everyone as if your facility were as important as a power plant.”

UNDERSTAND CYBERCRIMINALS

Imagine all hackers like this photo? The truth is much more sophisticated. While there are mischief makers who enjoy the fun of it, cybercriminals often have darker motivations. There are nation-states whose sole motivation is to disrupt, disillusion and demoralize a country. Those engaging in corporate espionage can seriously damage a brand. Many are simply chasing money, leaving a wake of chaos in their pursuit.

Courtesy of Tima Miroshnichenko / Pexels

"Those in it for profit are both the laziest and most persistent people in the world. They're looking for the path of least resistance," according to Fred Gordy, director of OT Risk Assessment with Michael Baker International. "If they send out 100,000 ransomware emails with a $10,000 decryption key and 1% are success, the takings are huge."

HOW COMMERCIAL BUILDINGS CAN BE WEAPONIZED

It doesn't take a sophisticated attack to cause mayhem in a commercial building, but it can easily have malicious outcomes.

HOSPITALS

Imagine a 20-story hospital with 1,000 IoT devices on every floor—that's 20,000 potential points of intrusion. Just turning off the lights or removing positive pressure could be catastrophic.

SPORTS AND ENTERTAINMENT VENUES

What would happen if someone hacked the jumbotron and posted an urgent evacuation message? It would take a few keystrokes to cause a stampede.

MANUFACTURING

The cost of shutting down a factory line is instantaneous. That's real money lost in seconds, much less hours. More importantly, this doesn't account for safety issues that occur from a sudden outage.

INDUSTRIAL FACILITIES AND LABORATORIES

Gases of all kinds are used and stored within buildings, especially those with scientific testing. The simple act of opening a valve to nitrogen, hydrogen, halon or natural gas could have fatal consequences.

Scenarios provided by Jim McGlone, CTO of Automation Strategy & Performance, Inc.

ID 204902773 © Nicoelnino | Dreamstime.com

How Property Managers Can Prevent Slips and Falls

Property professionals have a legal obligation to be proactive in addressing slip and fall risks, which can carry costly consequences for everyone involved.

By Tom Marsan

Over $70 billion is paid out every single year as a result of employee slips and falls. Falling is the No. 1 cause of accidental injury, and the No. 2 cause of accidental death in the United States, according to the WHO.

Property managers and owners have a legal obligation to be proactive in addressing the risk of falling, especially as the winter months approach. If risks aren't minimized, it could result in some costly consequences for everybody involved.

CAUSES OF SLIPS AND FALLS

There are four main reasons a person might slip or fall. While these reasons do seem to be fairly common sense, it's important to keep them in mind nonetheless.

Walkway Condition

When walking surfaces are slippery or wet, it can make people more prone to slips and falls. Additionally, if surfaces are uneven or contain changes in type, like a transition from a rough surface to a smooth surface, these differences can create hazard areas.

Courtesy of Beverly Companies

Walkway Changes

Steps, curbs or ramps can easily become a risky spot for many. The physically deficient, the ill or just the plain distracted walkers can all be a victim of a change in walkway.

External Conditions

Whether it's the lighting, the weather or temporary obstructions like a large tree branch, trips and falls can be increased depending on the external conditions.

Individual Circumstances

Reduced physical abilities, the choice of footwear and distractions such as mobile phone usage or navigating around others can increase the risk of slip, trip and fall incidents.

SOLUTIONS FOR SLIPS AND FALLS

While property managers and owners may not be able to eliminate all falls, there are certain steps they can take to ensure they are appropriately managing the risk of a slip and fall occurrence.

1. Training and Education

Properly trained staff members are a property manager's best asset in preventing slip and fall accidents. Regularly educate employees about winter safety protocols, such as the importance of wearing appropriate footwear, where to park and being aware of changing weather conditions. Highlight the hazard areas of the walkways with your staff to ensure everyone is adequately prepared.

As silly as it sounds to make mention of a curb or a transition from pavement to sidewalk, it will increase the mindfulness of the staff. Employee safety training should be an ongoing process, but it's also helpful if there is a written plan in place.

2. Snow and Ice Removal

According to many slip and fall studies—yes, it's probably not surprising that there are several councils and people devoted to studying this slipping and falling thing, 80% of slips and falls occur because of snow or ice. A strong majority of these incidents also take place in the morning hours.

If snow and ice removal is performed in-house, be prepared to be the first one in and the last one out during the winter months. Responsibilities should be assigned for monitoring forecasts, maintaining supplies of salt/sand, maintaining snow removal equipment and monitoring that the work is done well.

If you plan to find a company to battle the snow and ice for you, choose wisely. Snow and ice doesn't work on an 8 to 5 schedule and neither should a snow removal contractor. Find out how quickly they can be on site for a snow emergency by asking where their hubs and equipment are located and when they are available to salt or plow. Be sure to lay out an in-depth plan so everyone knows what to expect.

3. Anti-Slip Measures

Consider the lighting in parking lots and around walkways. Insufficient lighting during the winter can exacerbate slip and fall risks. Good visibility reduces the chances of accidents in icy conditions.

Anti slip mats should be at all entrances. These mats should include runners that extend further than the normal rugs that are used during the rest of the year as well. Mats will quickly become wet, and their effectiveness is void if there isn't an adequate space for wiping shoes.

Signs should be used to alert walkers of a wet walkway. As an added note to this end, buying a sign that utilizes humor is typically more effective than the normal caution sign. For instance, a sign that says "Caution, icy, walk like a penguin" will be more likely to grab the attention of walkers.

4. Emergency Preparedness

To be prepared for emergencies related to slip and fall occurrences, property managers should establish a comprehensive emergency response plan that outlines clear steps for assessing incidents, providing immediate assistance, and contacting appropriate medical help if necessary. This plan should be complemented by staff training in first aid and emergency procedures, as well as the maintenance of readily accessible first aid supplies and communication protocols for reporting incidents to emergency services.

Moreover, property managers should place a high importance on maintaining precise records of slip and fall incidents, along with the preventive actions implemented to reduce slip and fall hazards. Utilizing security cameras can assist in post-incident reviews following a slip and fall occurrence.

Property and facility managers play a pivotal role in maintaining safety during the winter months. By implementing proactive snow risk management strategies, they can create a safer environment for employees, visitors, and tenants while reducing potential liabilities. From snow and ice removal to employee training and emergency preparedness, these practical measures can make a significant difference in mitigating slip and fall risks. Stay ahead of the curve in snow risk management, and your property will be safer and more resilient during the winter season.

ADVANCE TO TOPICS

6 Ways Firefighter Air Replenishment Systems Benefit Commercial Building Owners

More states and Canadian provinces are requiring firefighter air replenishment systems (FARS) in buildings. What are they and how do they work?

By Mark Fessenden

Courtesy of Johnson Controls

In the United States, new high-rise apartments and office buildings continue to grow, along with massive warehouses and other large commercial structures. Part of managing these increasingly larger, more complex facilities is making sure the facilities have appropriate systems in place to help keep firefighters healthy and safe during emergency situations. This helps ensure the responding firefighters can focus on fire attack and helping to get occupants out of the building. Ready access to breathing air for the firefighters is key to this.

Historically, firefighters have had to hand-carry extra air canisters to have access to replenishing breathing air, which can slow fire attack response time. Firefighter Air Replenishment Systems (FARS) are a standpipe system for air, designed to provide a dependable and accessible source of air replenishment to first responders during a large structure fire. A network of pipes, valves and connections comprise the system, delivering air to designated fill stations strategically located throughout a building. FARS replace the slow, labor-intensive hand-delivery of replacement air bottles, both speeding fire attack and search and rescue operations and reducing the risk of exposure to the toxic effects of fire smoke.

As more U.S. states and Canadian provinces move to require FARS in buildings, it is important for building owners and managers to understand what FARS are, how they work, and how they can help keep their facilities prepared for an emergency situation.

Firefighter air replenishment systems (FARS) stations are designed to refill a self-contained breathing apparatus (SCBA) in up to two minutes, while the firefighter remains protected under full respiration.

Courtesy of Johnson Controls

HOW FARS WORKS

The system requires a dedicated air supply source, usually a high-capacity air compressor or air storage system. Air can be stored on-site or supplied by a fire department's mobile air unit. The FARS distribution network consists of a series of stainless-steel pipes that can run vertically or horizontally. Outlet connections, known as fill stations, are strategically located throughout the building. In a high-rise installation, they are typically located in stairwells where firefighters ascend and descend a building. In a tunnel or large horizontal structure, they are typically positioned adjacent to water standpipes.

Firefighters can activate the system simply by connecting their self-contained breathing apparatus (SCBA) bottles to the fill station outlets using tubing that is contained inside the fill panel. The system is designed to refill an SCBA in up to two minutes, while the firefighter remains protected under full respiration.

All FARS include an air monitoring system that tracks pressure levels and air quality. Regular maintenance and inspections are required by code to ensure that the system remains operational and in compliance with relevant standards and regulations.

6 LIFE SAFETY BENEFITS OF FARS

While FARS was designed to benefit firefighters and emergency responders, building owners also benefit from equipping their buildings with FARS.

Benefits include:

1. Enhanced occupant safety.
FARS ensures that firefighters have a readily available and continuous supply of breathing air throughout their operations. Lack of ready access to air will slow down critical fire attack operations, like search and rescue.

2. Faster fire suppression.
With a FARS in place, firefighters can refill their air cylinders and quickly return to fighting the fire. This puts more firefighters on-scene longer, increasing the speed with which they can suppress the flames.

3. Reduced property damage.
Fast, efficient air re-supply contributes to faster fire suppression and containment. The faster the fire can be controlled and extinguished, the lower the amount of property damage and the faster a property can be rehabbed.

4. Compliance with codes and standards.
Building codes and standards such as the International Fire Code and Uniform Plumbing Code include guidance on the installation and use of FARS in certain types of buildings. This guidance may be adopted by and turned into requirements for building construction by state and local communities. By implementing FARS, building owners can ensure compliance with requirements, avoiding potential penalties and legal issues.

5. Positive reputation and insurance benefits.
Insurance companies often take proactive measures into account when determining risk profiles and rates. Building owners who prioritize firefighter safety and invest in advanced fire protection systems like FARS can enhance their reputation as responsible and safety conscious. This can positively influence insurance premiums and coverage terms.

6. Relationship building with fire departments.
Implementing FARS demonstrates a commitment to supporting community safety, local fire departments and their firefighters. Building owners who provide FARS systems in their properties can develop a cooperative relationship with the fire department, leading to improved emergency response and potentially minimizing the impact of a fire incident on their property.

A FARS is a good example of innovative new building systems available to help firefighters and building owners alike. Designed to protect firefighters from the potentially deadly consequences of running out of air and breathing fire smoke, these systems can also benefit building owners, building occupants, and entire communities with enhanced protection, faster response times, and improved safety.

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.

By 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.

Courtesy of Genetec

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.

ADVANCE TO TOPICS

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.

5 Advancements of Next-Gen Access Control Systems

Amassing key cards and fobs on a lanyard are becoming a thing of the past as owners opt for newer technologies that offer more benefits.

By Andrew Froelich

Access control systems of yore were relatively simple technologies. An on-premises control server configured groups and users, who were then assigned a physical token, typically in the form of a key card. The system then centrally controlled access to all exterior doors along with a handful of highly sensitive areas, such as data centers, offices, conference rooms, and elevators.

In contrast, modern access control platforms are moving beyond the limited capabilities of centralized deployment architecture. New features expand the ease of use and effectiveness of a traditional physical security system. Lower component costs and flexible network connectivity options also enable the deployment of additional access-controlled areas within a building. In fact, modern access control systems offer five advancements that create value for both building owners and occupants.

Photo 209951069 © BiancoBlue | Dreamstime.com

SAAS ARCHITECTURE

Property owners are finding tremendous value in software as a service (SaaS) applications and services. Not only is a SaaS-based access control system a low-cost option in terms of capital and operating expenditures at scale, but it also eliminates the need to deploy and manage a physical access control server inside a local data center. This requires less data center space and eliminates the need to power and cool any in-house equipment.

SaaS-based access control systems are also incredibly scalable. Property IT departments can manage access to multiple buildings using a single management interface, simplifying system monitoring for companies overseeing several properties. Several SaaS-based platforms offer a smartphone app for users in lieu of a key card. This further eliminates any physical deployment of access control components, simplifying the onboarding and offboarding processes.

MICROLEVEL ACCESS CONTROL

Thanks to the lower cost of access control components along with improvements to connectivity options, including standard Ethernet, single-pair Ethernet (SPE), and Wi-Fi, adding door controller locks is easier than ever. The controller locks can secure interior doors, as well as cabinets, closets, and drawers.

BIOMETRICS

Biometrics, such as facial, voice, retina, and handprint recognition, are growing in popularity due to their decreasing technology costs and significantly improved accuracy in recent years. In many cases, biometric systems can eliminate the need for physical key cards. This removes the headache of forgotten or lost key cards while introducing touchless door access opportunities, a growing trend in a post COVID-19 world. This does raise privacy concerns, however.

MULTIFACTOR AUTHENTICATION

High-security buildings may require additional technologies prior to granting access to an employee, occupant, or contractor. Key cards are easily lost or stolen, leading to unauthorized access risks. To remedy this, owners can implement multifactor authentication. This security model requires the use of a physical token, such as a key card or cellphone, in conjunction with a biometric authentication method to provide added assurance that the person attempting to access a space using a physical token is indeed authorized to use it.

ANALYTICS AND INTEGRATIONS

The amount of useful data that can be extracted from modern access control systems is impressive. This information can determine who is accessing what, peak entry and exit times, and the flow of occupant traffic on any given day. Further data analysis can lead to deeper insights and actions, such as the following:

- Baseline normal access behavior at a per-user and per-group level. This information can be used to tighten role-based access policy and to identify potential security threats when access behavior veers significantly from the norm.

- Tie real-time occupancy location data to the HVAC system for more efficient control.

- Match occupancy numbers and location data with air quality and health-related IoT systems to improve the well-being of occupants in congested areas.

ROI OPPORTUNITIES ABOUND

Full replacement of a legacy access control system offers return on investment opportunities around every corner. Management simplification, automation, expansion of secure access points, and data-backed controls of HVAC systems to improve occupant health and operating efficiency are only the start of what can be accomplished.