A Supplement to Buildings, SIW, Security Business, Security Technology Executive

Supplement to *BUILDINGS, SIW, Security Business, Security Technology Executive*

JULY 2024

FACILITY SECURITY AND SAFETY MANAGEMENT TRENDS

Building the Modern Fortress

How to shore up physical security, cyber protection and more.

Security is just the beginning.

Leverage state-of-the-art AI to make your business even more efficient.

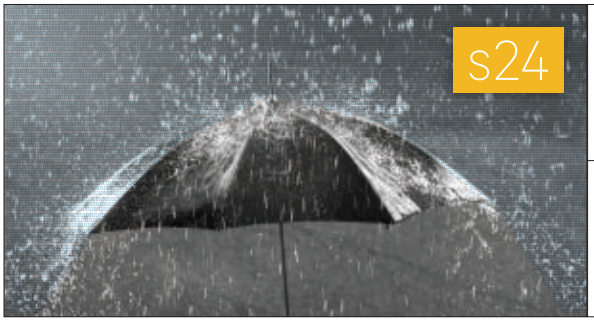
Revolutionize your building's video surveillance system with an open, true cloud platform and surveillance system using AI-enabled cameras.

Get peace of mind as well as valuable insights for efficient decision-making and process improvements. See how Eagle Eye Networks can change the game for your business.

SMART VIDEO SURVEILLANCE

Scan to learn more or visit een.com

EAGLE EYE NETWORKS



The Buyer's Guide to Cyber Insurance

What would you do if your organization or building was targeted by a cyberattack?

Read more

On the Cover
How to shore up physical security, cyber protection and more.

Composite illustration
Photo by Simone Hutsch on Unsplash
Photo by K. Mitch Hodge on Unsplash

Security By Design is a Proactive Buildings Security Strategy

This approach is a game-changer. It is a significant departure from the traditional approach of treating security as an afterthought.

Brivo, a leading provider of physical and cyber security solutions, recently conducted a survey. The results revealed that Security by Design, a concept that was not universally accepted, is steadily gaining traction among building designers. This emerging best practice involves planning for integrated security to be 'secure by design' from the outset. In other words, security features are incorporated into building blueprints during the design stage, just like heating and lighting are for comfort. This shift in approach is a testament to the growing recognition of the importance of security in building design.

'Security by Design' is not a mere reaction to the increasing complexity of threats, it's a proactive solution. By integrating security measures into the very fabric of a building's design and construction, this approach is a game-changer. It's a significant departure from the traditional approach of treating security as an afterthought. The benefits are twofold-it enhances security effectiveness and proves to be more cost-efficient in the long run.

The rise in cyber-physical threats is a key driver behind the adoption of 'Security by Design'. Modern buildings are brimming with smart technologies, from HVAC systems to lighting controls, all of which can be potential entry points for cyberattacks. By incorporating security measures from the outset, these vulnerabilities can be effectively mitigated, making 'Security by Design' a crucial strategy in the modern context.

Furthermore, the significance of Security by Design is underscored by the increasing focus of regulatory requirements and industry standards. For instance, frameworks like the General Data Protection Regulation (GDPR) and the National Institute of Standards and Technology (NIST) guidelines advocate for security to be an integral part of the design process. This not only aids in compliance but also plays a pivotal role in fostering trust with occupants and stakeholders.

The Brivo report states that despite the importance of security, it was, until recently, an afterthought in building design. Rather than considering security from the very beginning, it was addressed later. This meant costly retrofit efforts such as installing cameras to cover places with no natural surveillance, adding barriers such as planters where needed, and even adding security guard patrols. While we have learned to put thought into many other aspects of building design, such as heat, air conditioning, light, and elevators, security has not always been considered in the same way.

Today's growing security-by-design concept promotes a holistic approach to safety. It considers various aspects such as physical security, cybersecurity, and operational security, ensuring that all potential risks are addressed comprehensively. This integrated approach can lead to more resilient buildings better prepared to handle current and future threats. By embedding security into the design process, buildings can achieve higher protection and resilience.

Steve Lasky, Editorial Director

BUILDINGS

SECURITY INFOWATCH.COM

SECURITY BUSINESS
The Path to Greater Profits for Security Integrators

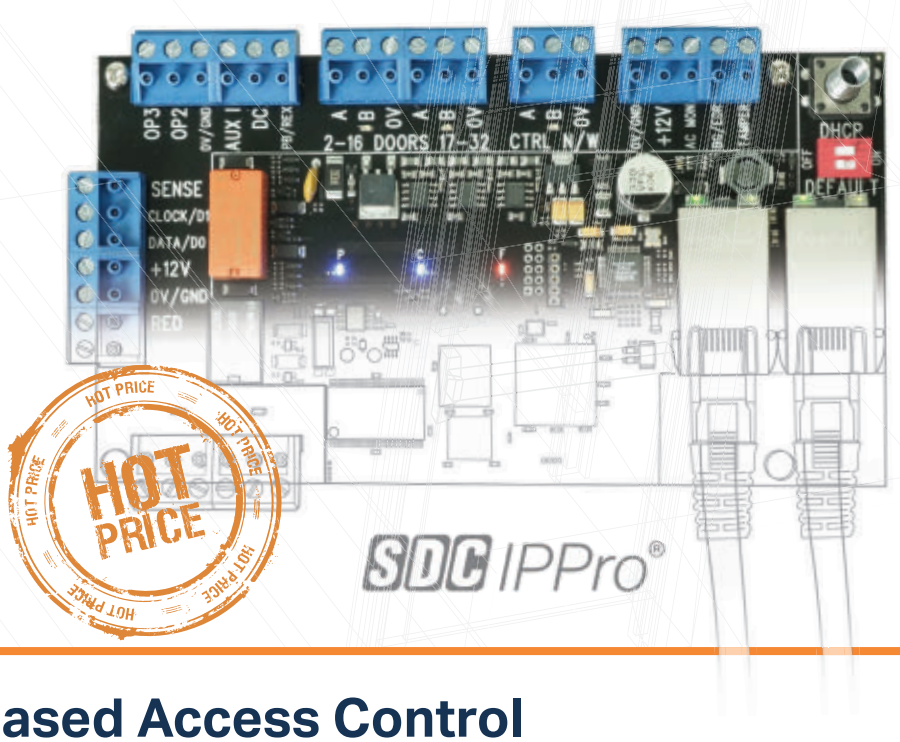
SECURITY TECHNOLOGY EXECUTIVE

BUILDINGS® (USPS Permit 070-480, ISSN 0007-3725 print, ISSN 2471-3112 online) is published quarterly in Q1, Q2, Q3, Q4 by Endeavor Business Media, LLC. 201 N Main St., 5th Floor, Fort Atkinson, WI 53538. Periodicals postage paid at Fort Atkinson, WI, and additional mailing offices.

POSTMASTER: Send address changes to: Buildings, PO Box 3257, Northbrook, IL 60065-3257.
SUBSCRIPTIONS: Publisher reserves the right to reject non-qualified subscriptions. Subscription prices, for all countries: $120 per year. All subscriptions are payable in U.S. funds. Send subscription inquiries to Buildings, PO Box 3257, Northbrook, IL 60065-3257. Customer service can be reached toll free: 877-382-9187 or at buildings@omeda.com for magazine subscription assistance/questions

NETWORK DOORS LIKE A PRO

Special Pricing Now Thru December 31st, 2024



Simple IP-Based Access Control

Integrate door openings easiliy into fully featured EAC systems without being an enterprise IT expert. **SDC IP Pro IPD Series** IP-based single door access controller is an ideal and economical solution for 1 - 8 door applications compared to enterprise systems. Avoid the headaches of costlier, more complicated enterprise systems.

PART#		DESCRIPTION	DEALER PRICE
IPDCE		IPPro Controller Board with Enclosure	$425
IPDSE		IPPro Door Station Expansion Board with Enclosure	$318

BUY NOW AT THESE PARTICIPATING DISTRIBUTORS

IML SECURITY SUPPLY · maglocks · JMAC · PSA SECURITY NETWORK

SDC Security Door Controls

the lock behind the system

sdcsecurity.com ▪ 800.413.8783

sdcsec.com/IPPromo

DESIGNED, ENGINEERED SINCE 1972 BUILT IN AMERICA

Lessons Learned: Security + Risk Roundtable

Workplace violence incidents are on the rise, but so are technologies that can combat it.

2021-2022

57,610

Assaults resulted in injuries (days away, restricted, or transferred cases)

2022

524

fatalities due to assault were reported

Rising concerns about workplace violence have increased demand for preventative and proactive security measures. But what can organizations do to implement a robust workplace violence prevention program? Concerns about legality, asset protection, and employee safety can be mitigated with the proper elements, including risk assessment, threat management, policy, documentation, and training, with each step involving every level of the organization.

Join host Steve Lasky alongside guests Charles Burns, Commercial Facilities Director, ISS; Matt Burke, Assistant Director of Safety and Security, BXP; and Rick Gross, President and CEO, Prometheus Security Group; as they discuss:

- Emerging threats facing facility security teams,
- The power of data and video analytics in ensuring safer and smarter buildings,
- Why AI and analytics are driving forces behind physical security convergence,
- And how to find the balance between a facility's security functionality and its aesthetic.

One of the largest concerns facing facility security teams is the rising tide of workplace violence incidents across the United States. Burke advocates for a collaborative approach when working with clients to understand it. Working with local law enforcement and property management agencies, alongside training in anticipation of emergencies, can do a lot to mitigate risk, reduce confusion, improve communication, and encourage faster response times in the event that a workplace violence incident occurs.

However, workplace violence is among a few emerging threats seeing the spotlight in building security. From a real estate perspective, Burke notes that accessible venues and emergency preparedness in major cities are major hurdles. "We need to ensure buildings remain secure while being able to respond to emergencies and unauthorized entry."

Burns raises the point that societal unrest is a major factor, especially in securing sports and entertainment venues. The geopolitical climate has made the threat of a protest or other incident foremost in the minds of many security teams.

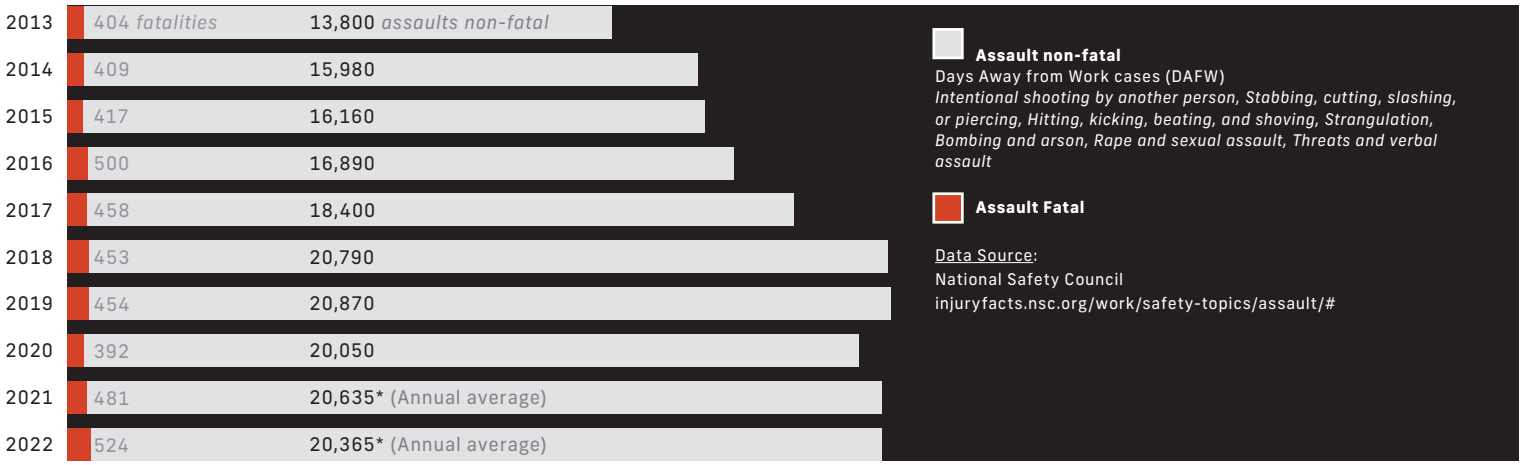
As a vendor, Gross leans more toward the usefulness of data in mitigating the prevalence of these issues. The convergence of physical security with the cloud has allowed physical security systems to generate a wealth of data based on their observations, and analyzing this data might serve to identify and mitigate potential security risks in the future.

The security convergence has brought security data analytics into the decision management process for a lot of facility teams, according to Burns. All teams need to participate in reporting to allow teams to make real-time decisions and reduce response times during emergencies. "Video intelligence in the decision-making process is a win-win for everyone," he says. "You need to bring everyone to the table."

According to Burke, the advent of video analytics is a game changer for the urban sphere. Legacy incident reporting systems couldn't collect data, so teams had difficulty identifying and predicting where to allocate resources. Now that they can, managers are able to integrate that data into their decision-making. "We're in the infancy stages of adopting video analytics, but it's here," he says.

This major migration to off-premises cloud has affected the way facility security is approached from the beginning, says Burke. The cloud reduces software updates, server maintenance, and power loads, so new buildings are designed with it in mind right out of the gate. The benefit of constantly available information is met with concerns about location and accessibility, though the invention of artificial intelligence to bolster analytics leads skeptics into the cloud regardless.

AI changes the way we look at the world and technology. The technology can be used to proactively improve workplace violence incident response by providing data that can help managers make preventative security decisions. Drone technology, which is also seeing increased implementation in facility environments, can provide organizations with valuable data lakes.



As a service provider, Burns emphasizes the importance of analytics to the decision-making process but that "communication is critical." Teams need to collectively monitor behavioral threat situations, collaborate across departments to analyze data and identify threats, and work together to define a comprehensive security approach.

Analytics can also play a role in the security environment battlefield. As buildings grow smarter and visitors increasingly expect certain systems and amenities, it becomes paramount for organizations to pay greater attention to balancing the aesthetic and functional aspects of their security systems. "You don't want to go through Fort Knox just to get into your office," Burke comments.

Buildings need to be traversable and secure without being cumbersome, so access control systems requiring entry point turnstiles, for example, can have a major negative impact on accessibility, traffic, and visitor experience. Areas with major obstructions can also prove dangerous or inefficient to navigate during emergencies.

Utilizing data analytics can provide security teams

with actionable intelligence regarding visitor traffic, behavioral patterns, and vulnerable locations, allowing professionals to more closely tailor their systems to their facility's needs. Critical areas can be shored up with additional security support and existing visitor management or access control systems can be streamlined to account for visitor behavioral patterns.

> "You don't want to go through Fort Knox just to get into your office."

While the data intelligence aspect of video analytics helps teams prepare or adapt their systems more adequately, preventative solutions utilizing video analytics include behavior analysis and weapon detection. Drawing from a database of trained information, these systems can identify signs of aggressive behavior or the brandishing of a weapon and notify security teams faster than a human observer. In this way, real-time monitoring of a specific threat can be attained without larger and less efficient physical security systems.

Burns speaks to the security of the upcoming Olympics, of which teams report a desire to keep venues as open as possible with attention to unobtrusive security methods. To maintain a security plan like theirs, he says, teams need to communicate, share intelligence, and, most importantly, make use of the most advanced technology at their disposal.

He relates this to facilities—no matter how open a venue or building appears, there is "never no security." Security technology is trending toward becoming more streamlined, efficient, and out of sight. According to Gross, you'll just need situational awareness and your head on a swivel to navigate it.

To learn more about how analytics can help security teams make their facilities more safe and secure amidst the threat of workplace violence, register to listen to the webinar at **www.securityinfowatch.com/55016849**.

by Samantha Schober, associate editor of SecurityInfoWatch.com

SECURITY + RISK PANEL

Rick Gross, President and CEO, Prometheus Security Group

Matt Burke, Assistant Director of Safety and Security, BXP

Charles Burns, Commercial Facilities Director, ISS

Secure every corner of your organization, across all sites

Find out how you can better monitor your organization, all while securing your people, and assets, and improving operations.

Genetec™

Visit genetec.com/pm

Security Center Synergis.

Emergency Preparedness for Facilities Comes in Myriad Forms

Emergency preparedness is as much about prevention as it is about business operations.

The prevalence of workplace violence and mass shootings have grown too prevalent for facilities professionals to avoid accountability for emergency preparedness. Every organization needs to have an action plan up its sleeve to ensure that its most critical assets, human lives included, are protected with every available resource.

Robert Nieminen, the Chief Content Director for EBM's Buildings/Architectural Group, moderated a panel with guests Sean Ahrens CPP, Security Market Group Leader, Affiliated Engineers, Inc. and Billy Cottle, Account Executive Enterprise, Genetec, Inc. as they discussed:

- The anatomy of an emergency response plan,
- Preventative and reactive strategies organizations can utilize during an incident,
- Why communication and training are key to employee and first responder safety,
- And what technologies are streamlining emergency preparedness.

The relative scarcity of emergency situations lulls many teams into a false sense of security they cannot afford. Ahrens concurs: "Security is only a 1% concern… until it is not."

He frames his point of view by comparing emergency preparedness in the workplace to the home. According to Ahrens, fires only occur in 0.2% of all homes, but most families have a fire exit plan in mind. Smoke alarms, sprinkler systems, fire extinguishers, and escape plans for children and pets are proactive aspects of emergency preparedness that can also translate outside of the home.

"Emergency preparedness is not just about operations; it's all about prevention as well," says Ahrens. "If you don't prepare for tomorrow's uncertainty and something occurs, you have a harder time recovering."

He advocates for mitigation through planning. Organizations can be held liable for any damage to assets or lives, so having contingencies in place is paramount. Crafting, applying, and testing an emergency plan is all you can do until one occurs. Afterward, teams must investigate the plan's response and efficacy during recovery.

Putting together a security plan begins with a tailored risk assessment. Ahrens emphasizes that every facility has site-specific risks, whether technological, biological, or man-made, that must be accounted for when designing an effective emergency plan. For example, if a facility houses machinery that could be damaged if not turned off properly, that asset is at risk if the emergency response plan does not account for it.

☑ KNOW YOUR CRITICAL ASSETS

Ahrens states that understanding asset criticality is the most important part of the planning process. Organizations need to understand which assets can be recovered and how quickly those can't be replaced. Lives cannot be replaced and are, therefore, the most important asset to protect. These priorities should inform all emergency response plans.

Once a thorough risk assessment is conducted, organizations can begin creating the framework for a flexible, scalable all-hazard plan as a baseline. Ahrens explains three fundamentals for building this plan: purpose, response, and recovery.

Purpose refers to managing critical assets during an emergency. Leaders, objectives, and mitigation strategies must be defined to best manage these assets. Language must be clear and concise to keep people informed and reduce response delays. Preventative strategies like employee training and emergency equipment should be accounted for when planning this step.

Employee training is one of the most vital prevention strategies available to organizations. All training should be tailored to the facility; some defensive strategies, like barricading doors, might impede emergency efforts in certain buildings. Tabletop and live-action plan testing is effective in these scenarios.

While an organization's facility-specific emergency response plan is an important starting point, there are other universal aspects of emergency training that can benefit teams. Teaching staff how to appropriately respond to both active shooters and law enforcement may prevent unsafe engagement with assailants and mitigate risk from accidental interference with law enforcement on the scene. Basic first aid may also save lives when first responders are unavailable.

The response includes elements of the plan that

PURPOSE	RESPONSE	RECOVERY
☑ DEFINE LEADERS	☑ ESTABLISHED COMMAND POSTS	☑ SHORT-TERM RECOVERY TARGETS
☑ OBJECTIVES	☑ LOCKDOWN PROCEDURES	☑ LONG-TERM RECOVERY TARGETS
☑ MITIGATION STRATEGIES	☑ EVACUATION ROUTES	☑ INSURANCE
☑ EMPLOYEE TRAINING	☑ COMMUNICATION SYSTEMS	☑ MEDIA PLAN
☑ EMERGENCY EQUIPMENT	☑ DEFENSIVE STRATEGIES	
☑ BASIC FIRST AID	☑ BARRICADING DOORS	

Photo 173208181 © Designer491 | Dreamstime.com

matter during the emergency itself. Established command posts, evacuation routes, and lockdown procedures are all aspects of active response. Ahrens emphasizes one, however: "The most important aspect of an emergency action plan is communication."

Establishing clear lines of communication via a facility's alarm, intercom, or mass notification systems encourages adherence to emergency plans, reduces panic, and can save critical moments when evacuating or sheltering.

> "The most important aspect of an emergency action plan is communication."

Direct communication with law enforcement and first responders allows them to better assess and prepare for the situation before they arrive.

Recovery after an emergency also needs to be considered. Short-term and long-term recovery targets, insurance, and media plans are practical aspects of recovery, but the efficacy of the emergency response plan in a real-world scenario also needs to be analyzed.

This includes the long-term effects on people, Ahrens notes. Insurance, length of work absences, and possible employee counseling are things that should be accounted for in the days immediately following an emergency.

☑ THE RIGHT DATA GUIDES EMERGENCY RESPONSE

Ensuring any emergency response plan is scalable to account for different kinds of incidents is also crucial, Ahrens states. While a wide range of emergencies can occur, a plan can still account for their similarities; he explains that shooters, for example, can be viewed as a "fire with cognition." While it is important to pen in a specific response and coordination strategy for active shooter incidents, establishing a uniform evacuation protocol might streamline the process, saving seconds that might be vital to defending assets or lives.

It is also imperative that security teams take stock of both internal and external data. Internally, data provided by integrated building security systems might offer actionable information on high-traffic areas or employee and visitor patterns. Externally, data collected by other organizations can provide teams with statistics on the most commonly attacked areas, average police response time and incident duration, and common event resolution scenarios that should inform their security plans.

Planning aside, buildings and the systems within them need to be constructed and integrated with emergency response in mind. Investing in shatter-resistant glass film and ensuring exterior doors lock is important, and, failing that, sheltering locations outside of the building need to be provided to ensure safe evacuation. However, technology is a "core element of emergency response," emphasizes Ahrens, with access control close behind.

Cottle agrees with this sentiment: "The use of these technologies not only enhances safety but also ensures quicker resumption of business operations post-emergency."

By assessing data as Ahrens encouraged, the importance of certain systems to a facility can be determined. According to statistics provided by Cottle, for example, 80% of school shootings occur outside of buildings. This implies that perimeter security and rapid response systems would bolster school security systems. Mass notification systems enable retail stores to evacuate up to 50% faster, and 62% of automated mustering systems cut headcount times during drills by an average of 25 minutes, saving time that could be crucial to protecting assets and lives.

Risk assessment and preventative action are crucial to preparing for the worst, as are the rapidly advancing technologies that enable swifter daily response. When crafting an airtight incident response plan, Cottle states that all teams should ask themselves, "How does your organization adapt its emergency preparedness strategies to protect both assets and human lives?"

Register for the webinar at **www.securityinfowatch.com/53098023** to learn more about the anatomy of an emergency response plan and the technology that makes it possible.

by Samantha Schober, associate editor of SecurityInfoWatch.com

EMERGENCY PREPAREDNESS AND YOUR BUILDING'S LIABILITY

Billy Cottle,
Account Executive Enterprise, Genetec, Inc.

Sean Ahrens CPP,
Security Market Group Leader, Affiliated Engineers, Inc.

Physical Security for Facility Managers Requires Multi-Level Approach

Building safety and security have been redefined in recent years and physical security systems need to keep pace.

Photo 117325157 © Pixinoo | Dreamstime.com

Physical security systems have not avoided the multiple technological upheavals the security industry has found itself combating in recent years. The movement to hybridize physical security systems has picked up a lot of steam, and now many individual capabilities, like video surveillance and access control, have been unified onto "single pane of glass" platforms. Now facilities are looking to integrate their security systems and marry asset protection to consumer experience, an approach that these experts hope to see catch on as buildings get smarter.

SecurityInfoWatch.com Editorial Director Steve Lasky joins guests Jarod Stockdale, Senior Project Manager and Security Consultant, Faith Group, LLC; Michael Niola, Senior Project Manager and Security SME, Faith Group, LLC; Darren Gonsalves, Account Executive, Enterprise, Genetec, Inc.; Rick Gross, President and CEO, Prometheus Security Group; and James Chong, Chairman of the Board, Advancis, Inc.; as they discuss:

- A step-by-step plan on security system assessment,
- Why collaborating with other non-security teams is crucial to improving security posture,
- How a smart security technology integrations can boost revenue,
- And what the analysis of security technology trends like IoT and automation can do to bolster both safety and customer retention.

A 5-STEP ASSESSMENT

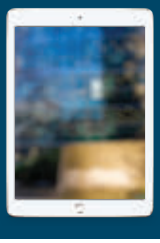
Niola and Stockdale advocate for a five-step approach to assessing a security system: setting security goals, understanding existing conditions, taking stock of security resources, assessing risk, and writing the "master plan." By their definition, a "master plan" is a strategic blueprint that addresses all aspects of a facility's technological functions, including operations, communications, business systems, and sustainability.

"The goal is to create a technology roadmap informed by current needs, future requirements, and evolving trends," says Stockdale. "The framework will serve as a North Star in prioritizing technology investments and optimizing performance in an evolving industry technology space."

"The first step is identifying security goals," Niola says. "What challenges are we trying to solve? How do our security systems affect overall business operations? Are we levering our current technology to the fullest?"

The technological goal of organizations in this phase is to make the most of existing systems and integrate them to meet defined use cases. Access control technology, for example, can be used to manage employee ID badges, while security camera footage can be analyzed to inform business decisions. For smart facilities, security technology can serve as a revenue booster, which further fosters collaboration with stakeholders.

> "Video surveillance and access control have been unified onto 'single pane of glass' platforms."



Other goals include increasing operational efficiency, providing more robust security training, standardizing security equipment, and implementing continuous evaluation and improvement cycles. Niola also advocates for organizations to push for the adoption of mobile credentials to support security, data, and revenue goals.

The second step is understanding your facility's existing conditions. This includes existing security, IT infrastructure, and a building's power and cooling systems. A building's existing security system can be repurposed, and understanding IT and security infrastructure makes potential future integrations less of a hassle. Site layout, doors, and room types are architectural aspects that can't be overlooked.

Next comes the analysis of the security team resources the facility already employs. All security stakeholders and what Niola calls "security champions" in other departments need to be identified. Security champions are advocates who can work interdepartmentally to advance security as a collaborative, rather than siloed, effort. Security is meant to provide value across an organization, Niola explains, so it is imperative that security teams remain well-represented. Procurement costs, including initial investment, operating costs, policy and training, must be identified when assessing resources an organization still needs.

Risk management is the fourth step of the planning process. Governance, Risk and Compliance (GRC) is vital, but Stockdale notes that having a local set of security standards and a plan to audit those standards is an easy way to streamline compliance. He also emphasizes that this is a collaborative effort between security professionals, employees, and shareholders.

"The more we interact and collaborate, the more we're able to leverage these systems into everyday operations," Stockdale says. "The more that we become integrated and involve non-security stakeholders, the more of an active role they have in decision-making and recognizing the value of these services."

When arriving at the planning phase, a thorough risk assessment is necessary to identify risks specific to a facility. All site data should be collected and analyzed to determine high-traffic areas or previously exploited vulnerabilities, and location-specific data like local crime statistics may help teams identify which incidents are more likely to occur.

RISK MITIGATION CRAFTS THE PLAN

Crafting this plan is all about risk mitigation, and the most effective way to begin mitigating risk is through employee training. This includes operational training, like keeping up to date on policies and procedures; technical training, which aligns operator capabilities with technology selections and allows for ongoing systems training; and tabletop exercises, which are an effective way of planning for incident response scenarios and testing their efficacy.

After the planning phase is over, teams should look at technology trends to select a security system, notes Stockdale. Technology is shifting toward biometrics and mobile credentials, proactive monitoring is becoming the industry standard with innovations like gunshot detection and real-time AI analysis of video feeds, and security systems are becoming integrated with each other.

Industry challenges typically feed security technology trends, so facilities can more easily meet the challenges of regulation, privacy compliance, and customer retention after identifying them. Studying trends like the widespread usage of IoT appliances alongside smart HVAC and lighting systems allows teams to identify customer standards and prepare for the risks of adopting them. Gonsalves champions this approach because it tackles several challenges simultaneously. Adopting technologies that customers expect to encounter, as well as technologies that enhance convenience and efficiency, helps ensure high satisfaction and retention, which is especially crucial for real estate management. Unifying technology helps facilities better gather and assess data, which feeds back into systems improvement.

Gonsalves says the increased attack surface inherent to IoT adoption can also be mitigated through inter-team collaboration. Interdepartmental collaboration with a "cyber mindset" can open a dialogue between operators, security teams, maintenance, and IT to rapidly identify and respond to potential vulnerabilities.

Threat and vulnerability management, access control, identity and video management, analytics, integrated security management, screening systems, and perimeter security are all integral to securing a smart building, Stockdale says, but automation is key to all of it.

Facility security is as much about improving the customer experience as it is protecting assets. Security automation can streamline the user experience while mitigating the risk to hospitality that comes with increasing security measures. "By automating many of these tasks, our businesses are evolving to become more effective, streamlined, efficient, and profitable," Stockdale states.

Register to listen to the webinar to learn more about leveraging smart and secure status to increase revenue: **www.securityinfowatch.com/55016829**.

by Samantha Schober, associate editor of SecurityInfoWatch.com

PHYSICAL SECURITY FOR FACILITY MANAGERS

Darren Gonsalves, Account Executive, Enterprise, Genetec

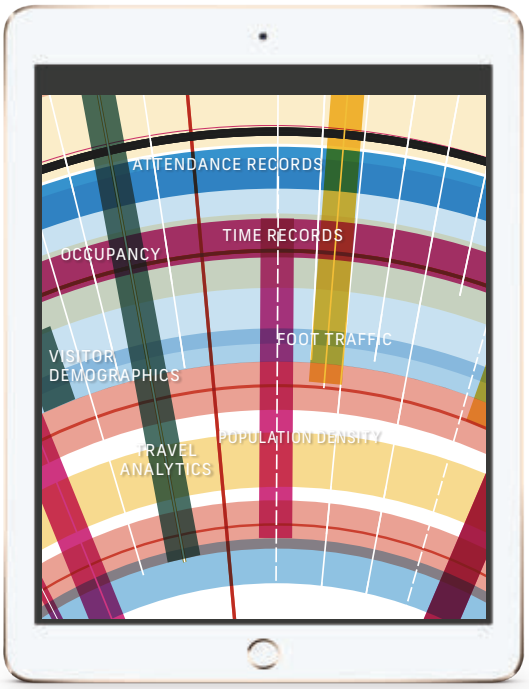
Jarod Stockdale, Senior Project Manager and Security Consultant, Faith Group

Rick Gross, President and CEO, Prometheus Security Group

James Chong, Chairman of the Board, Advancis, Inc

Michael Niola, Senior Project Manager and Security SME, Faith Group, LLC

What Is Proptech *and* *Why Security is a Key Element*



Proptech is white-hot, and many experts believe we have entered a new era in how commercial buildings operate.

2021

$32 billion

investment in Proptech

One of the largest and highest-performing categories in all venture capital markets.

Buildings and many of the devices they rely on are getting smarter. With a surge of investment money and increased interest in security streamlining and data collection, Proptech facility environments appear to be leading an industry-defining paradigm shift toward efficiency.

Expert guests Chris Wilson, Security Technology Market Leader, Mead & Hunt; Cameron Walker-Miller, Director of Standards and Technology, Security Industry Association (SIA); and Jason Lloyd, Regional Business Manager, ISS join SecurityInfoWatch.com Editorial Director Steve Lasky as they discuss:

- Why Proptech is seeing a boom in interest and investment,
- How to secure Proptech environments,
- The importance of Proptech's data collection capabilities to security and marketing teams,
- And how Proptech is ushering in a revolution in smart building management and consumer experience.

> "Real estate tech companies saw $32 billion in investments in 2021, making Proptech one of the largest and highest-performing categories in all venture capital markets. Walker-Miller believes this is a paradigm shift for building management."

WHAT IS PROPTECH?

Proptech, or property technology, is defined by Wilson as the technology connecting people and information to simplify how commercial real estate is owned, managed, operated, sold, researched, bought, rented, or invested in. Walker-Miller names Proptech as the technology facilitating real estate management, operations, and transactions.

Utilized throughout a real estate property's life cycle, Proptech can include emergency notification systems, fire and life safety systems, and audio detection. These systems are usually interconnected, and integration of these systems can streamline processes, reduce costs, and improve decision-making. However, this interconnectedness has the side effect of increasing an organization's attack surface.

"There are a lot of smart devices in these facilities that create convenience and operational efficiency," says Wilson. "We need to make sure security vulnerabilities are mitigated appropriately."

Wilson elaborates that Proptech environments are uniquely complex, so special care needs to be taken to secure them. Facilities using outdated or legacy security systems will likely find difficulty integrating these technologies and face interoperability challenges. The increased complexity and attack surface inherent to Proptech environments makes implementing and maintaining security measures challenging even after integration.

Because Proptech environments are so complex, qualified security professionals are needed to maintain them. A shortage of qualified security talent leaves a smaller pool of specialists up to the task, making it challenging for Proptech companies with smaller security budgets to shore up their defenses properly.

PROPTECH DRIVES CHANGE

Despite its challenges, investments in Proptech have catapulted it into the economic spotlight. According to the CRETI 2021 Real Estate Technology VC Report, real estate tech companies saw $32 billion in investments in 2021, making Proptech one of the largest and highest-performing categories in all venture capital markets. Walker-Miller believes this is a paradigm shift for building management.

"Proptech's importance stems from the ability to change how buildings are managed and the significant investments pouring into it," says Walker-Miller. "We're not just making changes when integrating Proptech with security solutions. We're sparking a shift toward making safer, more efficient, and more sustainable spaces."

Proptech's potential lies in its ability to streamline experiences for staff members, security teams, and customers. As a unified system spanning many devices, Proptech environments are highly flexible and can be easily tailored to individual preferences. Facilities with automation capabilities simplify property management and can streamline security processes. However, the straightforward applications of this technology are dwarfed by its ability to accumulate vast amounts of actionable data from across its device network.

Wilson says this data is the driver for system streamlining: "Data is what drives operational efficiency." Security teams can identify high-traffic areas, perimeter and system vulnerabilities, and locate specific users and assets within a building by utilizing the security data gathered from the multiple integrated IoT devices on the network, access control systems, or surveillance cameras.

While this data may help fortify a facility's security posture, building managers are interested in utilizing collected data for marketing purposes and to enhance the user experience. "Security solutions generate valuable data for various applications," says Walker-Miller. "Both security and Proptech companies are discovering opportunities to leverage each other's technologies for mutual benefit."

Walker-Miller offers access control as an example. Integrated access control solutions requiring cards or mobile credentials allow people to exit and enter the building as quickly and efficiently as possible, making things more secure and easier to manage.

DATA IS KING

Maintaining a secure access control system in this way is important, but the data that these solutions generate is the real point of interest. Population density, occupancy, travel analytics, foot traffic, time and attendance records, visitor demographics, and other actionable data is invaluable to marketing teams looking to entice new customers or improve the existing user experience. "It's not just about the mobile credential," says Wilson. "It's about interaction with the facility itself."

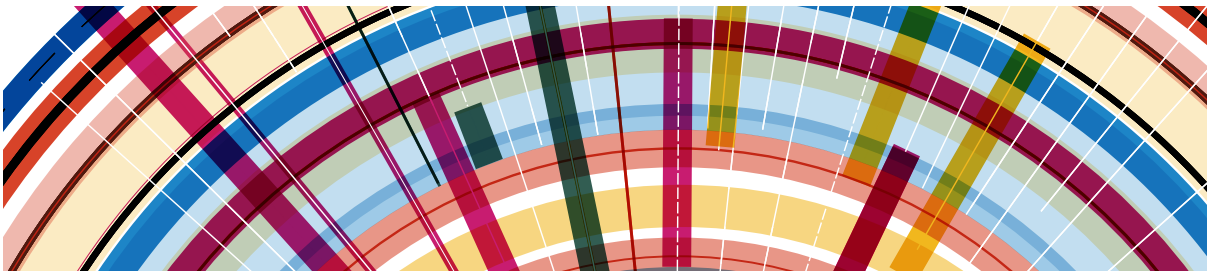
This is emblematic of the larger paradigm shift toward smart facilities evolving into "built environments", a term that encompasses the physical infrastructure, technology, and systems within buildings. Built environments do not ignore Proptech; rather, Proptech has transformed into an aspect of building management that the term encompasses. Walker-Miller notes this shift with the introduction of SIA's Built Environment Advisory Board, a body formed from SIA's former Proptech Advisory Board.

Wilson sees a bright future ahead for the built environment. As an emerging category, there is much room for collaboration between cybersecurity experts, Proptech companies, and industry regulators to develop best practices for engaging with technology. As these standards and expectations emerge, Proptech companies can work toward regular risk assessment and penetration testing to further improve their security posture. Additional advancements in young but rapidly evolving technologies like artificial intelligence, blockchain, and quantum computing will further enhance functionality and use cases, especially in building automation.

To secure a future for Proptech, an educated population is necessary, finishes Wilson. "Improved education and user awareness programs will empower practitioners and end-user clients to become active participants in using security devices as part of Proptech systems."

Register to listen to the webinar to learn how Proptech environments are elevating the smart building experience: **www.securityinfowatch.com/55016838**

by Samantha Schober, associate editor of SecurityInfoWatch.com



> "Proptech's potential lies in its ability to streamline experiences for staff members, security teams, and customers as a unified system spanning many devices."

WHAT IS PROPTECH AND WHY SECURITY IS A KEY ELEMENT

Jason Lloyd, Regional Business Manager, ISS

Chris Wilson, Security Technology Market Leader, Mead & Hunt

Cameron Walker-Miller, Director of Standards and Technology, Security Industry Association (SIA)

6 Benefits of

Operation centers are essential in risk management, continuously monitoring for potential threats.

As enterprise organizations grow—whether through organic growth or mergers and acquisitions—the scalability of the systems that keep them safe is called into question. A key component that becomes discussed centers around the ability of security teams to centralize operations, often within a security operations center (SOC) that allows for comprehensive command and control across multiple regions and teams.

Looking back on the years I spent at the helm of large-scale operations, SOCs were heavily used to pass information from one stakeholder or group of stakeholders to the next. During the COVID-19 pandemic, we were the centralized location for finding out information about infected colleagues and employee deaths. However, SOCs are being used to better understand how business is being conducted, as well as a centralized location for ensuring operations remain consistent. Centralizing this information in a single command-and-control environment is where the largest global enterprise security teams are headed.

The benefits of this are numerous, but here are some of the main ones:

STREAMLINED COMMUNICATION

There are few areas of an organization where information is shared more frequently or quickly than from a SOC. Monitoring not only unfolding internal incidents and events but also broader, more far-reaching global events (things like protests, conflicts, natural disasters) all fall within the realm of security operations. The reason is to protect people and assets from harm.

As such, the area of communication is a primary benefit of centralized command and control. Centralized systems allow for seamless communication between different security teams and departments—not to mention emergency response agencies, such as fire and rescue and the local authorities. The ability to quickly disseminate information and directives ensures that all personnel are on the same page during emergencies or routine operations.

CYBERSECURITY AWARENESS

Bringing together the cyber and physical security teams continues to be a goal that many large-scale, enterprise organizations are working toward. The ultimate goal for many of these teams is putting both departments in the same room to achieve what we call convergence, which is the bigger conversation. With all the incoming threats we have from both sides of the equation, and the amount of cloud-based, network-supported technology, it makes the most sense to have technology and security teams working together more cohesively.

Bringing the two together also has an element of compliance, including better mechanisms for logging activities, which can contribute to meeting legal and regulatory requirements. Having clear records of actions taken across the two departments enhances accountability and transparency within the security operations.

VALUE-DRIVEN INVESTMENTS

How can you articulate the value of a centralized SOC up the chain? If it's not done right, you may not get the resources you need to achieve your security department's goals. That's why focusing efforts on ensuring value-driven technology investments can make all the difference.

Centralized Enterprise Security Network Command and Control

A security operations center (SOC) allows for comprehensive command and control across multiple regions and teams.

Photo 312075716 | Screen
© Kjetil Kolbjornsrud | Dreamstime.com

One way this is done is by engaging with technology that is scalable. Scalability plays a big role in the success of centralized command and control, with forward-thinking organizations considering what growth means for their organization and planning accordingly. Too often, business leaders expand operations and grow organically without fully considering the organization's physical security. Ensuring investments in technology and resources can scale as the needs of the business change means driving more value for the organization in the long term.

Ultimately, security leadership needs to describe the value derived from technology investments in the same language the broader organization uses.

INFORMATION SHARING + VISIBILITY

Centralized command and control can integrate multiple systems into a single location, such as surveillance systems, sensors, and alarms, which provide a comprehensive overview of the broader security landscape of an organization. This level of visibility makes it easier for operators and analysts to engage in better decision-making, increase communication with internal and external resources (such as guards), and quickly identify and respond to incoming threats.

In a world where incidents happen so quickly, having a SOC that's staffed accordingly and armed with intelligence capabilities that have information from both physical and cyber security systems can help move the business forward and better protect assets. For so long, these same employees would have to pick up the phone and communicate, but now as we've entered this real-time expectation for information sharing, we're better equipped to protect our most valuable assets: the people.

COMPREHENSIVE RISK MANAGEMENT

Command and control centers are essential in risk management, continuously monitoring for potential threats and identifying vulnerabilities. Centralizing this function can mean quicker response to security breaches, and ongoing identification of threats. For example, advanced video intelligence driven by AI-powered analytics can help operators proactively respond to different security events. An organized protest that shuts down part of a route into a manufacturing facility, for example, can mean additional planning is needed in the event of an emergency where first responders are needed. Managing risk, these centers develop detailed emergency response plans, conduct regular drills, and maintain clear communication protocols to ensure preparedness for crises.

INCREASED COLLABORATION AND RESOURCE ALLOCATION

Centralized command and control enable security teams to better allocate and deploy security personnel and resources based on real-time needs and priorities. Having all the critical information and decision-makers in one place leads to quicker incident resolutions and reduces the time it takes to implement necessary actions.

Centralized SOCs offer benefits like streamlined communication and improved cybersecurity. By integrating cyber and physical security teams, they enable quick, coordinated responses to incidents. Value-driven investments in scalable technology support organizational growth, while comprehensive risk management and increased collaboration improve resource allocation and threat response, effectively protecting people and assets.

The final thought here is that organizations are going to grow, and they need scalable systems in place to do so. Centralizing command and control allows this to become a reality.

by Charles Burns, Director of Commercial Facilities, ISS

Strategies for Safeguarding Multi-site Enterprises

A holistic approach to standardizing physical security systems is critical.

In an era of unprecedented digital transformation, multi-site organizations face a myriad of challenges in standardizing and securing their physical security technologies globally. From stringent cybersecurity and privacy compliance requirements to the need to make actionable data readily accessible across the organization, the need for a reliable, experienced technology partner is paramount. A unified physical security platform combined with a tailored implementation can address large, multi-site enterprises' unique needs.

SEEK VENDORS WITH EXPERIENCE IN PHYSICAL SECURITY ACROSS MULTIPLE SITES

Multi-site organizations rely on physical security technologies to ensure business continuity across all of their sites and locations. Any disruptions or downtime to operations is a major security risk and can lead to million-dollar losses. Physical security systems must be operational even during system upgrades or improvements.

Some organizations might start upgrading one location and continue to expand from there. Others have a vision for unified and consistent operations at the start of the project. Regardless of the approach you decide to take, look for vendors who prioritize risk mitigation from project planning through deployment and beyond. Since you have multiple sites, your vendors must have the skills to support change management programs across all regions. Likewise, work with qualified and collaborative technology partners who can anticipate risks and have contingencies to ensure upgrades and migrations happen without any major issues.

Vendors who have multi-site experience can provide centralized coordination and local support throughout each project phase. They can coordinate with experts to assess project requirements, technical feasibility, risk mitigation, required customizations, roadmap planning, and more. Likewise, they often work with experienced local systems integrators to ensure a smooth deployment across all sites.

DEPLOYING MULTI-SITE PROCESSES WHILE COMPLYING WITH REGIONAL NORMS

Not only do multi-site businesses need to do everything they can to mitigate risks, but they also have to comply with increasingly stringent cybersecurity and privacy laws (i.e., GDPR, CCPA, HIPAA). If your organization has a large and widespread footprint, the complexity of compliance and the risk of breach are exponentially higher.

In many cases, large organizations lack the resources or visibility to adequately oversee firmware and software updates or track system vulnerabilities. As risks evolve, your team may require tools to help them standardize cybersecurity and privacy practices across your facilities while adapting systems and processes to local laws. Automation, unification, and additional guidance from trusted experts can enhance resilience.

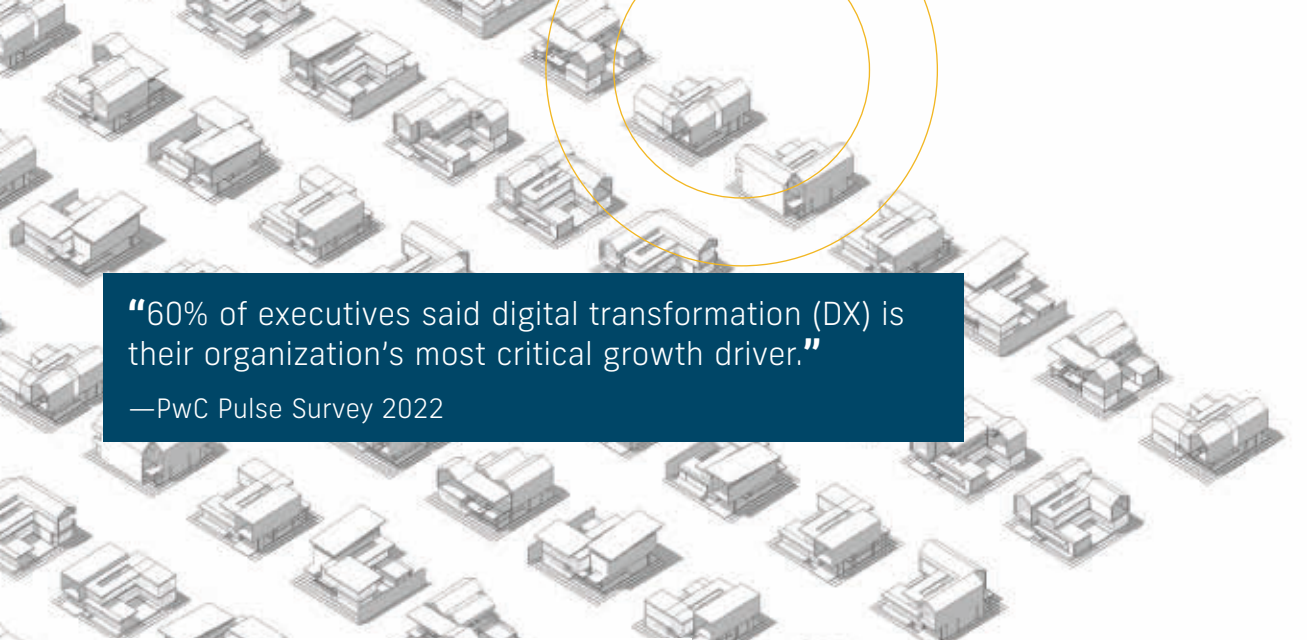
In addition to regulations, you may also have to consider different cultures, languages, and time zones. Choose a physical security platform that can be customized for each location's unique requirements while supporting standard operating procedures (SOPs). Regional flexibility helps strengthen resilience, compliance, and operator efficiency.

ENSURING OPERATOR PEAK EFFICIENCY AROUND THE WORLD

Standardizing a physical security solution is only one aspect. You also want to ensure that user adoption goes smoothly to maximize the value of your security investment. For this, you need more hands-on, personalized services and support. This might include relying on vendor experts to help with third-party integrations, system configurations, user training, or customizations. All of these efforts can help your team streamline operations and achieve greater efficiency and better outcomes.

Many multi-site security teams only use a small portion of their physical security systems' capabilities. Finding the time to learn the ins and outs of a security system can be tough and taking advantage of new tools and solutions often takes a backseat to daily security tasks.

To get more from your security investments,



> "60% of executives said digital transformation (DX) is their organization's most critical growth driver."
>
> —PwC Pulse Survey 2022

consider working with your manufacturer on specific customizations, hands-on user training and product certifications, and quick technical assistance. These tailored services pay off in the long term as your team benefits from built-in features, learns how to configure systems to boost efficiencies, and builds on what they already have by making small improvements along the way.

REDUCING THE COMPLEXITY OF MULTI-SYSTEM INTEGRATIONS

Large organizations often have legacy technology, hardware, and infrastructure that must co-exist with newer solutions. However, they also need to standardize the deployment and support. This can be particularly challenging when dealing with numerous regional channel partners or support contacts. A unified physical security platform based on an open architecture provides a way to connect to a vast ecosystem of technology partner solutions. These include access control, video management, perimeter detection, building automation, and third-party analytics.

An open platform can also support deployment flexibility with cloud or hybrid-cloud options. At sites with limited bandwidth, connectivity, or space, opting for cloud solutions can streamline upgrades and keep costs down. This way, no matter how your organization evolves, it will always have the flexibility and freedom to grow with the latest technologies.

UNLOCKING VALUE FROM SECURITY DATA TO ENHANCE OPERATIONS

According to the PwC Pulse Survey 2022, 60% of executives said digital transformation (DX) is their organization's most critical growth driver. As these DX initiatives expand, success relies on aggregating data from various sources and quickly making sense of the information to make informed decisions. Start by thinking more broadly about the role of physical security and related data. It can go beyond traditional applications to deliver more operational value.

Getting additional guidance from solution experts on supporting business needs is often the first step. You can capitalize on your security system investments to streamline new DX objectives. With a unified security platform, you can combine and analyze various data sources from physical security devices and Industrial Internet of Things (IIoT) sensors to uncover valuable insights and find opportunities to automate processes.

For example, you can track occupancy levels to meet evolving safety regulations or to evaluate office space usage. Bringing data from multiple sources and sites into one platform heightens your awareness of what's happening across your footprint. It also allows you to leverage the data to build unique applications that enhance decision-making and operations.

As IIoT continues to surge, you may want to achieve greater connectivity to applications, access information from multiple devices or locations, and manage larger amounts of data. The costs associated with managing and maintaining several systems add up quickly, often surpassing the initial costs of ownership. Thus, unifying your security and business systems and leveraging cloud capabilities will become vital as you streamline tasks and reduce costs, all while expanding IIoT connectivity.

SEEK OUT STRATEGIC PARTNERS

A unified approach is key in the fast-evolving landscape of multi-site enterprise security. From mitigating cybersecurity risks to complying with complex regional norms, multi-site organizations require more than just physical security technology. They need strategic manufacturer and systems integrator partners. A forward-thinking collaboration with a physical security systems partner will be the most cost-effective way to stay current in the long run. These partners must navigate the intricacies of standardizing physical security across diverse sites and ensure seamless deployment, user adoption, and ongoing support. Safeguarding multi-site enterprises requires a holistic approach tailored to your organization's unique challenges.

by David Ellis, Regional Director for Enterprise Solutions, Genetec

David Ellis, Regional Director for Enterprise Solutions, Genetec

Photo 101801650 © Kaspars Grinvalds | Dreamstime.com

The Threat from Within

Tips and tactics for building a world-class insider threat program.

The term "insider threat" conjures up images of rogue employees or malevolent spies infiltrating a high-profile organization to take it down from the inside. This can happen, of course—but insider threats can come from anywhere, in any size or type of organization, and can even include people who don't realize they are a threat.

An insider threat is simply someone who misuses their privileged access to organizational assets, causing either deliberate or accidental harm to the organization, explained Janet Lawless, CEO and founder of the Center for Threat Intelligence.

"Insider threats can be in any organization, no matter the industry, geography or size of the organization," she said. "It doesn't matter whether you have 100,000 people or two people—you can have an insider threat."

A solid insider threat program can prevent people from doing your organization irreparable harm, and it starts with a good foundation built on trust and training. Start by understanding the source of these threats, then shore up your prevention strategies.

UNDERSTAND INSIDER THREATS

There are several reasons why people target the organizations they are involved with, Lawless explained. Most insider threats fall into one of three broad categories.

- **Malicious:** The insider is acting with intent to harm your organization.
- **Compromised:** The insider didn't realize they were doing something wrong, but now someone is compromising them.
- **Negligent:** The person accidentally becomes an insider threat through means like a phishing attack, or even simply picking up a USB drive in your parking lot and accessing it to take a peek.

Malicious insider threats can be motivated by many possible reasons, Lawless added.

"Why does somebody want to target their organization? They could be disgruntled. They could have a loyalty to a nation-state. They could have medical expenses or a life change, such as a divorce, and suddenly they have financial issues," Lawless explained. "Life challenges can cause a good person to do bad things, depending on their particular situation."

Spotting this behavior in your organization can be difficult because there are so many potential reasons why people become insider threats, Lawless said. However, there are a few behaviors that should throw up a red flag for you.

- **Expressing grievances:** Employees may talk about the company being unfair because they weren't promoted or were denied a raise, noted Stefanie Drysdale, a Senior Vice President in Prescient's Cyber Practice. This isn't necessarily a red flag on its own, but it could indicate an opportunity to help a disgruntled employee.

Insider threats aren't always malicious individuals. They can be accidental—for example, an employee who picks up a USB drive in your parking lot and accesses it with their networked computer.

Photo 177763686 © Info723783 | Dreamstime.com

- **Straying out of their lane:** Is someone requesting privileges or access to parts of the building that aren't necessary to do their job? This could be another potential indicator that an employee may be acting as a threat.
- **Anomalous activity:** Employees who are suddenly logging in to your systems at strange times that aren't typical for them or exporting large amounts of data may merit further investigation, Drysdale said.
- **New contacts:** "We're seeing a lot of foreign adversaries on LinkedIn trying to obtain proprietary information from people who work for U.S. companies," Drysdale said. "Someone may accept all connection requests from unknown contacts on LinkedIn that are offering speaking or teaching opportunities in other countries. Those can ultimately lead to them selling data or giving up trade secrets."

"You can do an entire checklist of behavioral changes people may have, but the important thing to remember is just because somebody has a challenge doesn't mean they're going to become an insider threat," Lawless added. "You have to be very careful when you're looking at changes and behaviors and indicators that may be noticeable. But you also have to pay attention."

HOW TO START OR IMPROVE YOUR INSIDER THREAT PROGRAM

Building a world-class insider threat detection and mitigation program starts with having some hard conversations, Drysdale advised. What is your company doing now to detect threats from insiders? Will those solutions scale with you as your company grows? Explore resources from groups like the Cybersecurity & Infrastructure Security Agency (CISA) and the Department of Homeland Security to help guide these conversations.

Next, build your foundation by bringing in a consultant to help you understand your environment, challenges and risk profile. This consultant can assist you with hiring a program manager, conducting threat intelligence and behavioral psychology training, and building a strategy and framework.

"You should not hire an inexperienced person or a person who has no insider threat training," Lawless advised. "Hire somebody that has a background and experience [in it]. Sometimes those people are hard to find, so start with the consulting firm, get the foundation and have them help you look for the right person."

Insider threat prevention requires a company-wide effort, so you'll want to involve multiple departments from your organization as you build the program. The most important is your executive team, Lawless said: "The best way to fail in any program is to not have executive buy-in and approval." Your efforts might also include representatives from these groups, depending on the size and structure of your organization:

- The Board of Directors
- Human resources
- Legal
- Operations/facilities management
- IT

These departments should not be siloed at your organization, Drysdale said. Preventing insider threats and mitigating any potential damage is a group effort that demands a group approach.

"I've seen too many situations where you have very siloed organizations, and HR will be alerted that someone has been harassing a coworker. Maybe there is concerning behavior on social media, brandishing weapons or making threats. Maybe finance or HR knows about a garnishment or recent divorce," Drysdale explained. "If those are very siloed and departments aren't sharing intel, then it's just one anomalous thing—the guy's grumpy or going through something. If you put it all together, then perhaps there's opportunity to step in and provide support before this person becomes an insider threat."

Once you've built the foundation, training for everyone can begin. Threat prevention is the job of every employee—if someone sees something, you want them to say something. Everyone needs training so they know what they're looking for. However, it's critically important that you approach this training with the intent to educate, not crack down on people making mistakes.

"When you come with a benevolent viewpoint, you

Christopher Burgess,
Security Consultant,
Former Senior Security Advisor, Cisco Systems

Janet Lawless,
CEO and founder. Center for Threat Intelligence

Stefanie Drysdale,
Senior Vice President,
Prescient's Cyber Practice

avoid creating an incident where none exists. Lots of folks forget that," said Christopher Burgess, security consultant and former senior security advisor to Cisco Systems. "For example, the company wants to teach about phishing and says, 'If an employee clicks three times, I'm getting rid of them.' So, you put all this money into this employee, hired them, trained them, put them on the job, and now because you created a very creative email that fooled them, you're going to get rid of them—and then you give yourself a gold star for fooling your own employees. How about you come up with a different solution that if the employee clicks, nothing bad happens?"

> "The tone at the top and supporting employees is very important. It's got to come from the top."

Training should cover the knowledge that your organization is maintaining activity logs and monitoring physical and online activities, Burgess added. Be upfront about saying your building has surveillance and you're monitoring what people do on your network. "Then there are no surprises and everyone expects it," Burgess said. "If you manage the expectations—this is what we're doing and why we're doing it—then the individual knows their expectation of performance and behavior. The weakest link is ambiguity."

SUSTAIN AND GROW YOUR PROGRAM

Your insider threat program will require constant effort to make sure it not only continues but thrives. Sometimes, insider threat prevention can fall victim to budget cuts because it's hard to prove a return on investment for avoiding harm. Executive approval and involvement are paramount to keeping the program going, Lawless said. Make sure you're constantly reporting results to your executive team, so they understand the value of the program.

"Every time an employee helps another employee out, that's a metric. Every time your IT team stops something from happening inadvertently, like a file being shared with a competitor, that's a metric. Every time an employee raises their hand and says 'If we do it this way, it might be more secure than the way we've been doing it,' that's a metric," Burgess said. "The metrics aren't going to jump off the page as 'I saved this many opportunities for information to be stolen.' The metrics are going to be that you have employee retention, morale is high, you have fewer mistakes that put information at risk and you're heading off behavior before it manifests itself as negative behavior because your employee assistance program is there as your safety net."

Company culture plays a huge role in preventing insider threats by instilling loyalty and building an environment where people feel safe reporting potential issues. People may still make mistakes that put the company at risk, but a healthy culture can cut down significantly on disgruntled employees who want to harm the company on purpose. "When people are loyal, they go out of their way to make sure the entity is protected," Burgess said.

4 TOP TAKEAWAYS

Building an insider threat program is hard work, no matter whether you're building it from the ground up or improving an existing program. Remember these four key takeaways as you shape your threat detection and mitigation practices.

1. Don't forget the human aspect of security. Technology can help you discover anomalous behavior, but it can't tell you why employees are behaving that way. Don't jump to conclusions—investigate before you declare that someone is behaving threateningly.

"It's important to realize that if someone has come online, and they don't usually get online after 7:00 at night and suddenly they're getting inline at 2:00 in the morning, the tools are going to say, 'Here's a red flag. Somebody's accessing critical information at 2 a.m.,'" Lawless explained. "As you do more background investigations, you may find that they just had a baby, and the baby may be keeping them up at night, so they could be awake and getting some work done at 2 a.m. It's important to use the technology, but also use the human aspect to understand the context and intent."

2. Create a culture of trust. "The tone at the top and supporting employees is very important," Lawless said. "It's got to come from the top."

3. Always include legal. "You want to make sure the rights of your employees are respected," Lawless said.

4. Educate after mistakes. Some insider threats start as a mistake—someone clicks on something they shouldn't have, for example. Insider risk management helps catch these mistakes. "You need to have the ability to recognize the state where the mistake is made. Have an in-the-moment rectification and education," Burgess said. "When you have an incident, take the position of benevolence, not malevolence as the motivator—the individual was trying to do the right thing, but did it poorly."

Stopping insider threats before they do permanent damage to your organization is a team effort, Drysdale added. The more you can shape your culture so everyone is rowing in the same direction, the better off your program will be.

"Have the messaging going into it that we are all invested together," Drysdale said. "Having an insider threat program is an opportunity to prevent [threats] and continue to do the good work you do, to build and grow."

by Janelle Penny, Editor-in-Chief, BUILDINGS

SECURITY BEYOND THE CAMERA LENS

Scene Authentication: industry's first Zero Trust Architecture (ZTA) instantly detects breaches, video spoofing, and data manipulation at the edge

Proves imagery from: "THAT Camera - THAT Location - THAT Point in Time"

Scene Authentication:

- Cost Effective
- FED-GOV vetted, patented technology
- PKI and encrypting the scene to the enterprise
- Verifiable video data allows advanced AI/ML analysis
- Enhances response teams' safety and success

Available for Distribution, Private Label and Licensing. IAW Presidential Executive Order (EO) 14028

PROMETHEUS
SECURITY GROUP GLOBAL
Industry's Zero Trust Engine

psgglobal.net

LinkedIn (512) 247-3700

NDAA Compliant | TAA COMPLIANT | GSA Contract Holder

Buyer's Guide to Cyber Insurance

Is your property covered?
Here's why you need comprehensive cyber insurance—and how to shop for it.

2025

$10.5 trillion

Cybercrime costs

Cybercrime is expected to account for $10.5 trillion in losses globally by 2025, according to a report from the research firm Cybersecurity Ventures.

What would you do if your organization or building was targeted by a cyberattack?
Do you have cyber insurance that would step in?

And more importantly—are you sure your cyber insurance is comprehensive enough to protect you?

Any business or building that's connected to the Internet in any way is vulnerable to a cyberattack. Every organization needs a comprehensive cyber insurance policy that's tailored to their unique needs.

Here's how to make sure you have the right policy for you—and how to shop for it if you don't.

WHY IS CYBER INSURANCE SO IMPORTANT?

Cybercrime is expected to account for $10.5 trillion in losses globally by 2025, according to a report from the research firm Cybersecurity Ventures. The threat is growing. That's why cyber insurance is such a crucial tool for anyone who owns or operates commercial real estate.

"Insurance is there to protect you when you have an unexpected bad day. Cyber attacks are almost always unexpected," explained Dan Burke, senior vice president and national cyber practice leader for Woodruff Sawyer, one of the largest independent insurance brokerage and consulting firms in the U.S. "To me, the value of insurance is having something there to protect you when you weren't expecting to pay for a cyber security attack or the fallout from an attack."

Buildings and organizations are most commonly vulnerable to two types of cyberattacks, according to Burke:

1. Funds transfer fraud. "Think about building owners and tenants. There's often money going around back and forth between these groups," Burke said. "Attackers have devised ways to insert themselves into that money transfer process, whereby they trick humans into sending money to the attackers instead of where it was supposed to go."

Bad actors can gain access to your email and network and watch and learn for a while, Burke explained. "They can see with whom you're interacting or transferring money, and then at some point, they insert themselves and redirect that money into their bank accounts. It happens all the time," Burke said. "The number one most common cyber attack we see is funds transfer fraud. It's a very prominent risk for building owners."

2. Ransomware. "Every company that's connected to the Internet is exposed to ransomware risk, and it can be

devastating," Burke said. "It can shut down essentially all access to any sort of networking services that require access to a network of any kind."

That includes not just your Internet access, but any connected building systems, from access badges to elevators, explained Jason Lund, managing director for JLL Inc. "If the vendor can run, fix or troubleshoot a system remotely from their headquarters, which you want them to be able to do, that also means somebody can hijack that system," Lund said. "If somebody can run it remotely, someone can hack it."

Ransomware encrypts your network and disables your access to connected systems until you either pay the ransom or restore your systems from backups, Burke added.

HOW CYBER INSURANCE PROTECTS BUILDINGS

Cyber insurance steps in if these attacks happen—if you have cyber insurance. In the last five years or so, insurance around cyber risk has evolved quickly, Burke said.

"Many carriers now have affirmative coverage or affirmative exclusions on almost every insurance policy when it comes to the impact of a cyber event," Burke said. "Because of this, commercial insurance policies almost exclusively exclude cyber claims, and they force that coverage into a dedicated cyber insurance policy. If you don't buy a dedicated cyber insurance policy, it's unlikely you're going to have coverage for a cyber security event."

Your cyber insurance policy will protect you in two key ways, Lund said. "In order to get the cyber insurance, they're going to make you jump through a bunch of hoops and tighten up your security," he explained. "If you do have insurance and something bad happens, you'll be able to recoup some portion of your monetary loss."

In the case of funds transfer fraud, for example, your insurance carrier will help you alert the authorities and either recover the money or reimburse you (up to a limit) for the amount you lost. If you fall victim to ransomware, your insurance provider can help in several ways, including bringing in experts you'll need to help you recover. These include:

- Breach counsel, who will help if you're sued in connection with the ransomware event and assist in contracting with other vendors who need to get involved
- Cyber forensics experts, who can determine what went wrong, how the attackers got into your systems and whether they still have access, and what systems or files were wrongfully accessed and how
- Ransom negotiators, who will negotiate the ransom down to a lower number (potentially buying you time to restore your systems from a backup and avoid paying the ransom altogether)

Cyber Insurance Buying Basics

There are a few basics that every cyber insurance policy should cover, according to the Federal Trade Commission. They include:

- ☐ Data breaches, like incidents involving theft of personal information
- ☐ Cyber attacks on your data held by vendors and other third parties
- ☐ Cyber attacks, like breaches of your network
- ☐ Attacks that occur anywhere in the world (not only in the United States)
- ☐ Terrorist acts

A good policy will include both first-party and third-party cyber coverage. First-party coverage protects your data, including your employee and customer information. It typically covers the costs you would have to pay out of pocket to recover from a cyberattack, such as:

- ☐ Business costs related to legal counsel
- ☐ Recovering and replacing lost or stolen data
- ☐ Customer notification and call center services
- ☐ Lost income caused by business interruption
- ☐ Crisis management and public relations costs
- ☐ Cyber extortion and fraud
- ☐ Forensic services
- ☐ Fines, fees, or penalties related to the incident

Third-party coverage steps in to protect you from liability if a third party brings claims against you, according to the FTC. This should cover:

- ☐ Payments to customers affected by the breach
- ☐ Claims and settlement expenses relating to disputes or lawsuits
- ☐ Losses related to defamation and copyright or trademark infringement
- ☐ Costs for litigation and responding to regulatory inquiries
- ☐ Other settlements, damages and judgments
- ☐ Accounting costs

> "If the vendor can run, fix or troubleshoot a system remotely from their headquarters, that also means somebody can hijack that system."

Jason Lund,
Managing Director, JLL Inc

Dan Burke,
Senior Vice President and National Cyber Practice Leader, Woodruff Sawyer

IS YOUR POLICY RIGHT FOR YOUR PROPERTY?

In addition to the basics, you'll want to make sure your policy is tailored to your organization and, if necessary, individual properties. Some property types, like healthcare, are more heavily regulated and will have certain requirements for cyber insurance. When you're talking to brokers, you should also consider things like:

- What is my property type?
- How much is my property worth?
- How much does my organization rely on technology to operate and generate money?
- If that technology fails or is inaccessible, how much money could we lose?
- How many connected building systems do I have, and what could happen if they're compromised?
- Are there people involved in my assets who are especially vulnerable, like residents of a skilled nursing facility?

"If you have an asset worth a lot of money in a major market, or a lot of people going in and out—especially vulnerable people—you should investigate very seriously with an insurance company or a broker," Lund said. "They can help you."

Ideally, that broker should have specialist experience in cyber insurance, Burke recommended. Expertise in cyber insurance can make a major difference when it comes to tailoring your coverage.

"The biggest thing you're buying when you buy insurance is somebody who's actually going to be there for you, not looking for a way out," Burke said. "To me, a reputable broker is where you start."

3 STEPS TO TAKE RIGHT NOW

Before you sign on the dotted line for a new policy, make sure you have covered the basics by taking these three starter steps.

1. Check your current policy.

Many insurers have moved away from covering cyber threats as part of a larger property insurance policy; you most likely need separate coverage for cyber insurance. "Do you have cyber insurance, and if so, what does it consist of? Make sure you know," Lund advised. "Don't just read the policy that you bought five to seven years ago—call your insurance company and have them look up your policy and tell you what your current coverage is for cyber. Review exactly where your coverage is, even if the written policy is in front of you and get on the path to gaining cyber insurance."

2. Understand the exclusions.

Even a comprehensive cyber insurance policy won't cover everything. Many companies believe lost value from trade secrets will be covered, but it isn't, Burke said. That's because it's impossible to quantify the loss in value to insure against it.

"The loss in value of your company is not recoverable under cyber insurance," Burke added. "That's the biggest one people get confused about. … You can get coverage for responding to that event and how the trade secrets are stolen, but you cannot recover the lost value of your company."

3. Shore up your security practices.

Understand how building systems are monitored, both within the building and remotely by service providers and vendors, Lund urged. What cyber security protections do your providers have in place to protect you? "More and more, we're starting to see in contracts with vendors, if they're going to be doing remote access, do they have insurance for cyber, and does that sit in front of our insurance? It should," Lund said. "You're bringing a service into our building, and if it gets hacked and damaged, we want the vendor to be responsible and do the cleanup. That's good protocol from the building owner's standpoint."

The right policy for your property and organization will be tailored according to your unique risk profile. It will ensure that your business can recover if it's targeted by a cyberattack, and it will complement your security staff's hard work by helping you identify practices and policies that can be improved.

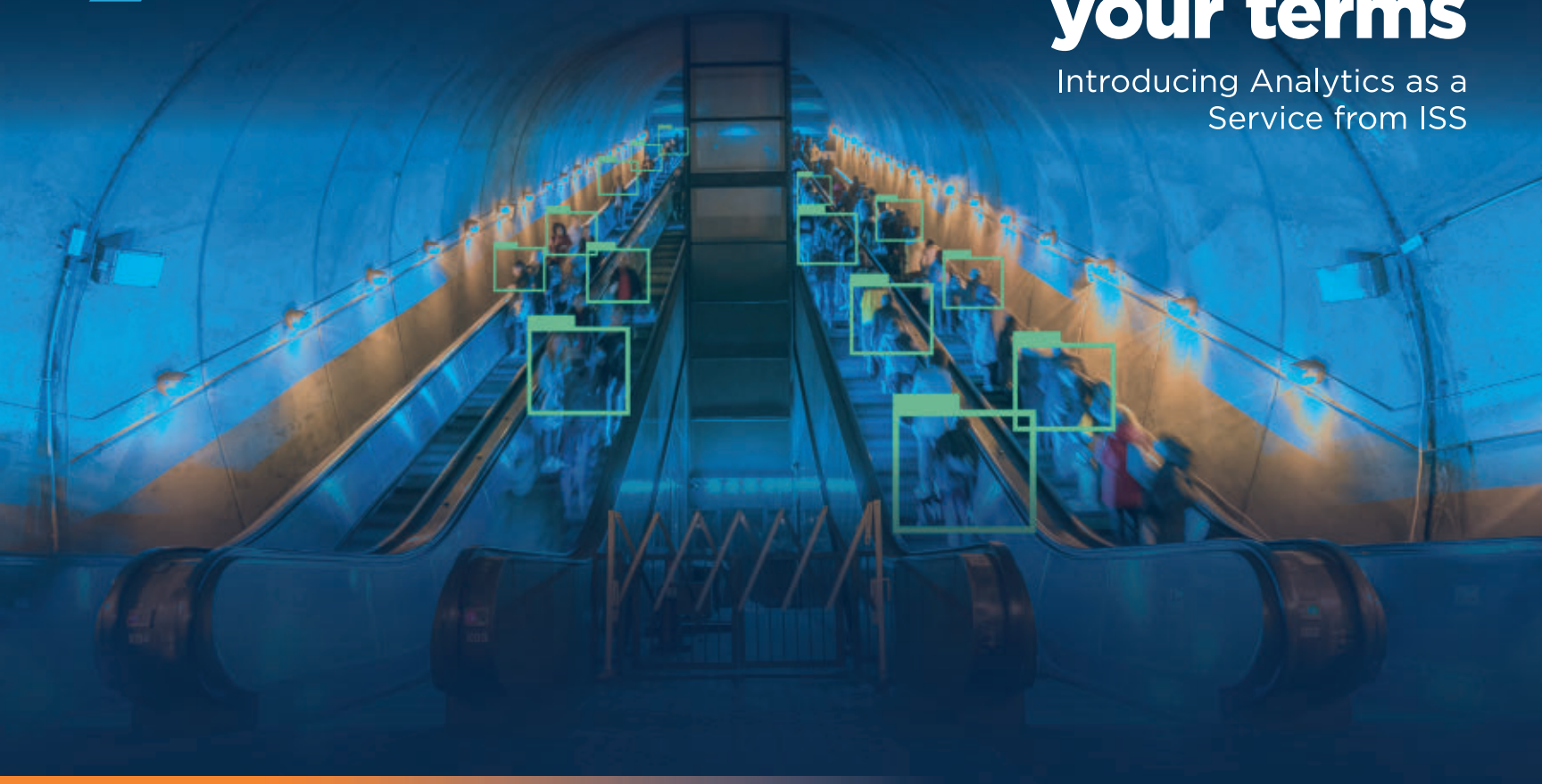
"Cyber insurance as an industry is here to support you in your security efforts," Burke said. "We are very much on your team when it comes to protecting your organization, making you whole and getting you back to business faster."

by Janelle Penny, Editor-in-Chief, BUILDINGS

ISS
INTELLIGENT VIDEO. DEFINED.

AI on your terms

Introducing Analytics as a Service from ISS



Unlock the power of **video intelligence** with our new Analytics-as-a-Service offering, revolutionizing the way organizations harness data for enhanced decision making. Our a-la-carte, **no hardware required** approach allows you to pick the specific analytics modules that align with your objectives, tailoring the service to suit your exact needs. Whether you're focused on traffic flow optimization on a local roadway or PPE compliance in a manufacturing facility, our platform puts a comprehensive selection of analytic tools at your disposal.

Upload a Free Clip Today!

Scan the QR Code to Ask Us How!

Available Analytics Include:
People Counting // Weapons Detection // Fighting Detection //Fallen Person Detection // Vehicle Counting // License Plate Recognition // PPE Detection // Turnstile Evasion // Vandalism Detection // And much more!