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

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

JULY 2025

FACILITY SECURITY AND SAFETY MANAGEMENT TRENDS

The convergence of physical security, building automation, and facilities operations

table of contents

Read more:

On the Cover
The convergence of physical security, building automation, and facilities operations.

Credit: metamorworks 1255556729 iStock / Getty Images Plus

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

Holistic Strategies for Integrating Physical Security into Building Automation Projects are Critical

Managing a building is about more than operating efficiently. Safety and security must be integrated from day one.

The creative and editorial staff of Endeavor Business Media's Security and Buildings groups have collaborated on what has become an annual project to share the expertise of facilities and security management practitioners and experts in demonstrating the importance of an open working environment when it comes to ensuring the safety and security of America's buildings and institutions.

Modern buildings demand more than just efficient operations; they require integrated safety and security as part of their core infrastructure. As physical security systems, such as advanced access control, intelligent video surveillance, AI-powered analytics, and emergency communication tools, become more sophisticated, they must be fully integrated into building automation projects. Achieving this requires a coordinated strategy involving security, facility management, and building operations from the outset.

A holistic security integration strategy delivers several mission-critical advantages. First, it enables real-time situational awareness across building systems, which is vital for emergency response, incident prevention, and risk mitigation. For instance, by linking access control systems with video analytics and AI-based behavioral detection tools, security teams can proactively identify anomalies and threats before they escalate. Similarly, integrating these technologies with HVAC and lighting systems can help automate lockdown protocols or evacuation responses, thereby increasing the speed and effectiveness of emergency communication and life safety measures.

Second, an integrated strategy supports operational efficiency and long-term cost savings. When physical security solutions are implemented in silos, the result is often overlapping technologies, redundant infrastructure, and disparate data sources. However, unified platforms that share intelligence across building automation systems can streamline maintenance, reduce energy consumption, and optimize staffing by automating routine tasks and monitoring performance in real-time.

Crucially, collaboration across departments ensures that the solution architecture is designed to meet all functional requirements, not just those of the security team. Facility managers can help align security infrastructure with broader building performance goals, such as energy efficiency and smart space utilization. At the same time, IT and cybersecurity personnel can address the risks inherent in network-connected devices and cloud-based platforms, ensuring compliance with internal policies and industry regulations.

To maximize these benefits, building owners and project teams must view security not as a cost center but as a strategic enabler of business continuity, occupant experience, and operational excellence. By adopting a holistic approach to physical security integration within the broader building automation framework, organizations can future-proof their facilities, improve resilience, and foster a safer, smarter, and more sustainable built environment.

Steve Lasky, Editorial Director, EBM Security Group

BUILDINGS

SIW SECURITY INFOWATCH.COM

SECURITY BUSINESS
The Path to Greater Profits for Security Integrators

SECURITY TECHNOLOGY EXECUTIVE

How Will AI Maximize Your Building's Security and Business Operations in 2025?

Artificial intelligence can help manage building security—but it's not without its challenges.

by Samantha Schober

Artificial intelligence (AI) has quickly evolved into a technology we'd once consider the realm of science fiction, but its impact is very real. AI has already revolutionized several industries with demonstrable impact on security, operational efficiency, and ROI, and it's up to today's professionals to maximize its value.

Janelle Penny, Editor-in-Chief of *BUILDINGS*, guides **Lauris Freidenfelds**, Vice President of Security Risk Consulting at Telgian Engineering & Consulting, and **Jason Ouellette**, Corporate VP of Innovation and Technical Partnerships at ELATEC, through a discussion about:

- Emerging AI technologies and the ways in which they bolster both security and return on investment (ROI),
- The new (and familiar) challenges that come with integrating AI technologies into your operational ecosystem,
- And what AI means for the future of security, whether an organization implements it or not.

THE ROI OF EMERGING TECHNOLOGIES

The sudden abundance of new AI technologies has had a measurable impact on the ways industry professionals are managing and securing their buildings. The five most "transformative," Ouellette explains, are these: predictive maintenance, smart surveillance, energy optimization, operational efficiency, and the usage of digital twins for simulations.

Predictive maintenance, for example, enables users to utilize AI to detect and address issues with equipment before they cost organizations time and money. Teams can use AI's automation capabilities to simplify routine tasks and redirect personnel toward more critical work. Optimizing systems involved with HVAC or lighting promotes efficiency and helps meet sustainability goals. Simulation tools and digital twins build virtual environments for testing before implementation, potentially saving money and reducing planning load.

"AI is a force multiplier," says Freidenfelds. "You can use fewer staff to accomplish more with technology. Information is processed quickly, so we can respond faster and more accurately."

The security implications of AI, Freidenfelds emphasizes, are enormous. "Video systems used to be forensic tools," he says. "Now we're using analytics and AI in real time. It's a shift from reactive to proactive security."

Today's unified security ecosystems have a commonality to point to, he says: AI. AI has streamlined the integration of video surveillance, access control, intrusion detection, and weapons detection, helping to eliminate security silos and facilitate a shift toward proactive risk mitigation.

Because AI software can be introduced at the "edge" (for example, through a smart camera) and at the "head end" (via software overlays), it is very easy to integrate into larger security ecosystems without replacing legacy infrastructure. However, it is crucial that organizations looking to upgrade their systems perform the proper audits to determine both optimization and compatibility.

Ouellette urges organizations to "start small" with pilot programs before leaping into large-scale deployments: "Don't try to boil the ocean." Freidenfelds concurs with the notion that upgrades must be strategic to promote cost savings: "Assess what you have and identify what you can use. You don't have to throw the baby out with the bathwater."

IMPLEMENTATION CHALLENGES

While integrating AI technologies has reduced some challenges, it has also introduced new problems. The largest pitfall, according to Ouellette, is strategy.

"The biggest challenge to AI adoption is the lack of clear strategy," explains Ouellette. "AI should align with your business goals. Otherwise, you're just adding complexity."

Freidenfelds emphasizes that these technologies are intelligent and evolving and must be treated as such—they must be "managed, not mounted."

This is an especially important step when working within legacy systems. Planning is required when determining whether existing infrastructure is compatible with AI technologies to prevent overspending when it comes to actually bridging the gap.

Another concern is data quality. AI models aren't all-knowing—they are only as intelligent as the data they are trained on. If that data is flawed, biased, or otherwise inaccurate, the integrity of both the AI model and the technologies it powers are compromised. To ensure the integrity of training datasets, a robust data governance framework is essential.

"Transparency and explainability in AI systems are logical," explains Ouellette. "If the logic behind decisions isn't clear, you risk ethical missteps and regulatory trouble."

Organizations looking to adopt AI technologies must take these ethical and regulatory considerations into account. Illinois' recent Biometric Information Privacy Act (BIPA), for example, places heavy restrictions on the usage of facial recognition technologies and other biometrics.

To comply with regulations like these, Freidenfelds emphasizes

that less is more—collect as little data as possible to reduce the risk of misuse. Additionally, organizations must be able to understand their AI models: why they come to the conclusions they do and if that conclusion was reached via biased or otherwise discriminatory data.

The final major hurdle is the tendency of people to resist change. Just as with cyber-physical convergence before it, many feel overwhelmed by these sophisticated new technologies. Others fear their employment status may be threatened by the potential of AI to automate many aspects of their day-to-day. The answer? Education.

AI, when utilized correctly, has the potential to significantly enhance an employee's capabilities. Effective communication and training enable workers to both understand what their AI tools can do for them and what they can do to increase the efficiency of these tools. Existing staff roles can then be reallocated to areas that require critical attention.

Regardless of the challenges, Ouellette says that organizations need to adapt to this new environment or risk being left behind. "AI-driven surveillance and anomaly detection across all systems will explode," he explains. "We're just scratching the surface today."

THE FUTURE OF AI

This "explosion" of AI technologies in building systems is inevitable, Ouellette says. As cyber and physical security continue on their path of convergence, the higher number of connected IoT devices in a facility will knock cybersecurity up the priority scale. AI will become critical to preemptively detecting and responding to cyber threats that target these devices.

As security systems become more unified, AI will be a crucial factor in proactively predicting and targeting various scenarios. By combining and integrating diverse data from multiple sources—such as access logs, video feeds, or legal databases—threat actors and security incidents can be identified and mitigated before they occur.

If organizations want to take advantage of this security shift, however, they need to be proactive as well. Freidenfelds recommends working with a trusted advisor or consultant to assess what value an organization is looking to extract with AI technologies and how those technologies slot into existing systems. This multi-year roadmap should include staggered AI integrations, pilot projects, and staff training programs.

Regardless of AI's benefits, some organizations simply may not be ready to adopt the technology yet. Even if implementation is further down the road, Ouellette says, there are still steps that can be taken to improve your overall security hygiene and lay the foundation for future upgrades.

"Even without AI, start with better password hygiene, multi-factor authentication, and regular audits," Ouellette says. "That's the foundation."

Whether an organization takes steps to adopt AI technologies or not, its existence will impact them in some way. The opportunities AI offers to enhance and streamline building operations and security are incredibly significant, but implementation efforts depend on comprehensive planning, ethical implementation, and continuous system support.

Even with the complexity involved in integrating advanced AI systems for security, Freidenfelds concludes that the goal is as simple as it ever was: "Make people feel safe."

Register to listen to the full webinar here:
www.securityinfowatch.com/55278950

Samantha Schober is associate editor of **SecurityInfoWatch.com**.

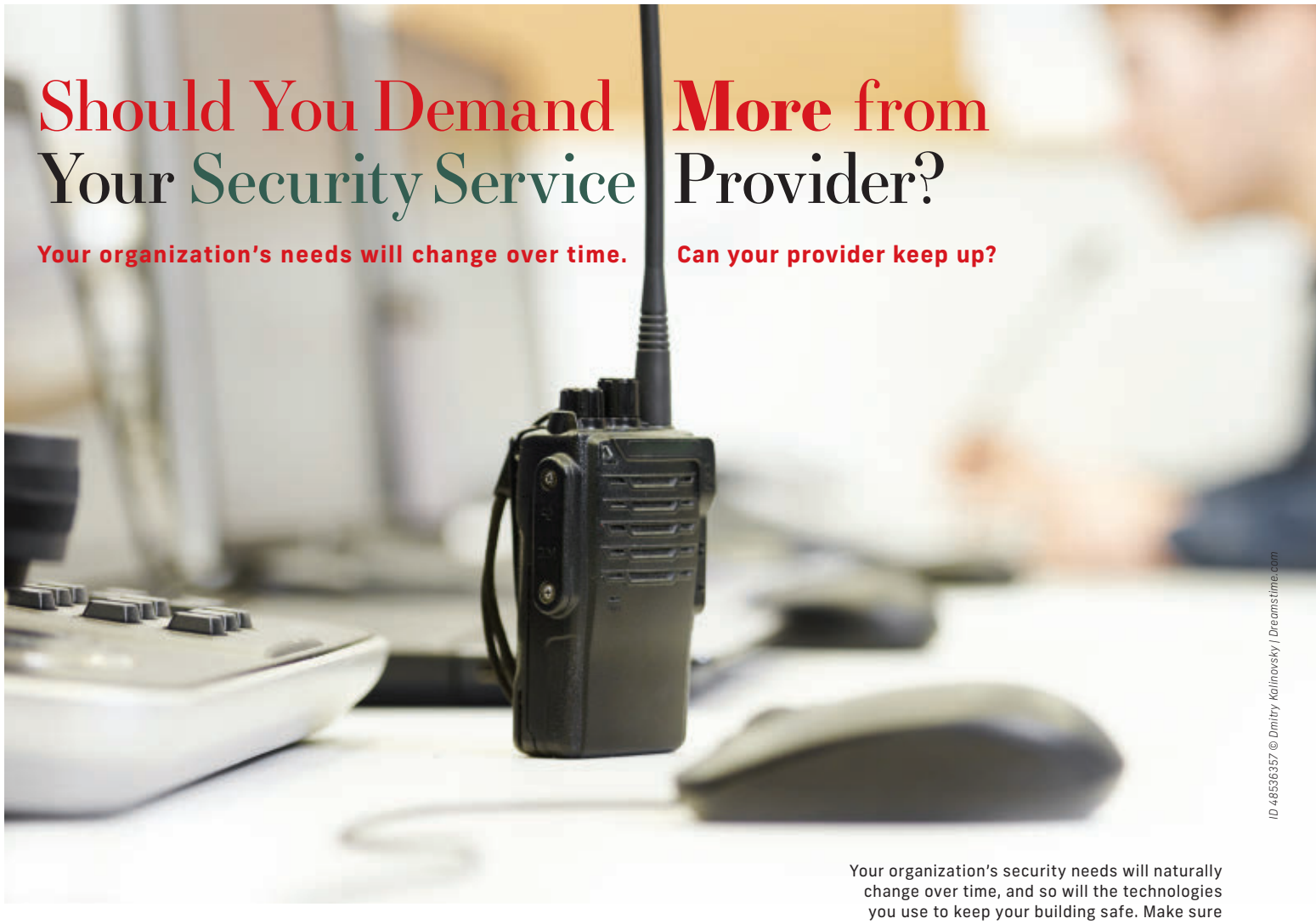
WEBINAR PANEL

Jason Ouellette, Corporate VP of Innovation and Technical Partnerships at ELATEC

Lauris Freidenfelds, Vice President of Security Risk Consulting at Telgian Engineering & Consulting

Should You Demand More from Your Security Service Provider?

Your organization's needs will change over time. Can your provider keep up?



ID 48536357 © Dmitry Kalinovsky | Dreamstime.com

Your organization's security needs will naturally change over time, and so will the technologies you use to keep your building safe. Make sure your security provider is positioned to meet your needs now and into the future.

by Samantha Schober

In an era of rapid technological change, organizations must adapt to keep up. But internal assessments are not the only way to promote progress. As the needs of your organization evolve, it is important to reassess whether your current security services provider can rise to meet them.

Security Technology Executive Editor-in-Chief **Steve Lasky** invites **Rob Hile**, Sales Manager at GC&E Systems Group, and **Shaun Castillo**, Pref-Tech's President, to offer their insights on:

- The importance of keeping accountability within partnerships a two-way street,
- The impact that evolving technologies, industry consolidation, and economic uncertainty have on client relationships and integrators,
- And what the future looks like for the survival of both clients and security providers.

ENSURING ACCOUNTABILITY—BOTH WAYS

Ensuring that your security service provider is aligned to the current needs of your organization is crucial to maintaining a fruitful partnership. Hile and Castillo suggest using key performance indicators (KPIs) to measure provider performance but also emphasize that these metrics should be shared with clients via proactive discussion.

"Set clear expectations from the beginning," Castillo says. "Too often, we're never told how we'll be measured until things go wrong."

These metrics can cover a vast spectrum, from response times and communication frequency to past performance and transparency, especially with finances. Other critical benchmarks, especially post-COVID, are inventory management and change order frequency.

However, this relationship must be a two-way street: "Customers have skin in the game too," says Hile. Providers must be evaluated, but so should customers. A customer grading system for communication habits, payment timing, transparency, and clarity offers insight into which clients to engage with.

"We did an analysis and found that the top 20% of our customers generated over 90% of our revenue and profit," says Castillo. "Those customers care about relationships, trust, and

long-term engagement. That's who we prioritize."

Hile stresses, however, that there is no "one-size-fits-all" KPI or service agreement. "SLAs (Service Level Agreements) must reflect each customer's mission, urgency, and expectations. You tailor response levels and communication plans to match."

SLAs should be tailored to each client's needs, service mission, and operations. Response times, communication protocols based on geography and issue severity, and maintenance expectations are a few of the most common elements. Castillo, however, emphasizes the importance of clarity in ensuring customers understand what their expectations actually cost. A two-hour emergency response across a metro, for example, requires high-cost infrastructure that must be reflected in the final price.

"All strong relationships are built on clear boundaries," says Castillo. "Figure out what your customer really needs and what it realistically costs to deliver that."

Communication is a critical determining factor when it comes to ensuring projects are completed and deadlines are met without a compromise in quality. This and education are critical to collaboration in a technology ecosystem that is changing too quickly to keep up with.

NAVIGATING INNOVATION AND ECONOMIC CHANGE

Artificial intelligence (AI), IoT, and cloud-based security solutions are firmly in the driver's seat of today's tech environment. Security service providers are often expected to keep up with this rapid innovation while also educating their customers, who may not fully understand how it works.

Castillo's solution to this issue was the building of Pref-Tech's "innovation team." Pref-Tech's innovation team evaluates and pilots new technologies before customer deployment, reducing risk and ensuring smooth implementation. Working in conjunction with key clients can potentially save them millions of dollars. "Every dollar spent with us is an investment, and we have to prove that investment was worth it," Castillo explains.

Hile also emphasizes the importance of maintaining strong ties with manufacturers and integrators to keep them ahead of the technology curve. The heightened popularity of cloud-based systems presents significant revenue challenges for integrators, who must contend with reduced revenue from traditional on-premises system maintenance.

Financial transparency with integrators, Hile notes, is key. Unviable or unsustainable solutions must be clearly communicated to the integrator so they can find the best way to provide value. "Cloud is amazing, but it's killing integrator margins," he says. "It disrupts the integrator model. This isn't sustainable unless we adapt—and we are."

Technology, however, isn't the only driver of our turbulent economic climate. Global trade disruptions—including the fluctuating tariffs—are straining relationships between supply chains and vendors. Consolidation within the industry has led to service degradation in some cases, causing lapses in consumer trust.

To navigate these relationships successfully, proactive communication must be established to rebuild trust in the industry. "Talk to your clients about tariffs," Castillo says. "Maybe we order early to avoid a spike. We negotiate. Transparency helps us all manage risk."

Hile advocates for questioning surcharges and requiring detailed justifications to shield customers from unnecessary spending. "Fight for your customer—it pays off," he says. "If we don't evolve together, we don't survive."

> **"The security industry is undergoing an economic and technological upheaval."**

One of the ways organizations can increase customer trust—and satisfaction—is to have high levels of employee engagement and a robust company culture.

"Customer satisfaction won't exceed employee satisfaction," explains Castillo. "Invest in your people, train them, and engage them. That's how you deliver great service."

THE FUTURE OF SECURITY INTEGRATION

The security industry is undergoing an economic and technological upheaval, and to Hile, the tech side of this revolution is very apparent: "The big three are technology intelligence, cloud services, and cyber awareness. With more devices and remote access, converged cyber-physical security is no longer an option."

Disruptive cloud services will continue to grow and demand business innovation. Cyber-physical convergence, with the advent of AI analytics and automation, is already here with the demand that security systems must remain compliant and cyber-hardened. This spills over into the workforce, as organizations are already finding it difficult to attract and retain employees with relevant technical skills.

"Your tech can be cutting-edge, but if your people don't care, it all breaks down," Hile explains. "Finding the right people is harder than the tech."

Castillo names another economic pressure on the workforce: the rising influence of public equity (PE). "The elephant in the room is private equity. It's everywhere—changing expectations, rushing ROI, and undermining service quality. The 3-year ROI model doesn't fit customers looking for 10-year reliability. They are noticing, and so are we."

The only way to weather this storm is to remain adaptable and transparent. Maintaining an open dialogue will be the deciding factor in how both clients and security providers succeed moving forward.

Register to listen to the full webinar here: **www.securityinfowatch.com/55278971**

Samantha Schober is associate editor of **SecurityInfoWatch.com**.

WEBINAR PANEL

Rob Hile,
Sales Manager,
GC&E Systems Group

Shaun Castillo,
President, Pref-Tech

What Are the Hot Security Technologies Your Facility Manager *Should* Consider?

These emerging tech trends are changing the way security is managed.

by Samantha Schober

Smarter buildings demand smarter approaches to security. Emerging technologies are redefining the way organizations protect and manage their facilities, from AI-driven automation and video surveillance to mobile credentials and biometrics. Early adopters of these technologies are already deploying them to reshape how they respond to risk.

John Polly, Chief Solutions Officer at ProTecht Solutions Partners, and Faith Group's Senior Project Manager & Security Consultant **Jarod Stockdale** join **Steve Lasky**, Editor-in-Chief of *Security Technology Executive*, to explore:

- The new security technology trends taking the industry by storm,
- How to look past the hype at actual use cases for new technologies,
- And why future-proofing your systems is a critical, ongoing process.

As buildings become increasingly connected, the silos that have historically separated facility managers and security teams have begun to break.

"Security is no longer just a siloed function—it's a cog in the wheel of the organization," says Polly. "It enables HR, marketing, and facilities to solve problems using our tools."

Facility and security teams must collaborate when it comes to adopting new technologies, he elaborates. Teams must break down traditional communication barriers, share data, jointly plan projects and roadmaps, and ensure that they are aligned on core operational goals.

NEW TECHNOLOGIES ON THE HORIZON

Security leaders and building operators have a wealth of new technologies to choose from once their plans are in motion.

AI is one of the largest game-changers for smart buildings. Repetitive tasks that teams used to have to perform manually can now be automated by AI, like credential resets or video footage analysis. This enables organizations to reroute staff to more important tasks.

The only thing as well known as AI, however, are its risks. Users must evaluate their training models, remain transparent, and clearly define their use cases. However, Polly notes, those willing to lead the charge in AI adoption will reap the benefits: "Big risks can mean big ROI. You just need to ask, are we ready to be a leader, or are we going to wait and follow?"

Mobile credentials are the latest trend in access control technology because of the flexibility and security they offer as compared to physical badges or keys. They can be remotely issued and revoked, offer time-based permissions, and be integrated into smartphones. Enabling mobile access control reduces the necessity of on-site key handovers, provides temporary access for visitors or maintenance staff, and enhances security via encrypted communications.

Perhaps more important than its use cases, however, is the shift in expectations. New generations in the workforce are not interested in conforming to traditional access control systems, Polly says: "Younger employees are saying, 'My phone is my badge. I've never carried a badge, and I'm not going to start now.'"

> "Innovation does not always correlate with success. 'The best technology in the world for the wrong use case is the wrong technology.'"

Sustainability initiatives targeting plastic cards are also making a push toward standardizing mobile credentials.

Digital twins—real-time models of physical structures or locations—have become a new way for teams to map their facilities. Through this interface, organizations can optimize their energy consumption and promote sustainability via real-time updates, simulate emergency scenarios, or perform predictive maintenance to identify and remedy problems with infrastructure before they get worse

Stockdale offers a real-world example: By identifying actual occupancy levels, teams can scale power usage to the number of people in the building, which is especially useful for large multipurpose buildings like shopping malls.

"Digital twin technology is not just security," adds Polly. "It's business intelligence that can reduce energy use and improve occupant experience."

Global Security Operations Centers (GSOCs) are proliferating across the industry and are often adopted by resource-strained organizations like schools and churches in an "as-a-service" model. They provide faster incident response and alarm verification and centralize control for distributed sites. "It's the difference between a frantic call from a night guard and a verified alert from a professional operator," says Stockdale.

Third-party GSOCs, Polly notes, are also seeing usage as "stopgaps" while organizations migrate new acquisitions into their networks. "With constant acquisitions, GSOCs are becoming permanent solutions," he adds.

hxyume 1409023759 E+ Getty

Enabling mobile access control reduces the necessity of on-site key handovers, provides temporary access for visitors or maintenance staff, and enhances security via encrypted communications.

Converged IoT systems are becoming the industry standard. Most modern facility ecosystems contain IoT technologies like card readers and HVAC units that are already connected to the internet.

The popularity of these systems is undeniably ease of use—integrating these devices into the whole improves visibility across systems and enables automation of routine tasks and controls. However, integrating more IoT devices creates a larger attack surface, potentially exposing networks to opportunistic hackers. Some of these devices may also lack the proper isolation protocols to prevent them from connecting to the cloud by default.

"We talk about convergence, but sometimes we forget to ask if a device was vetted or isolated," says Stockdale. "That's where the blind spots start."

USEFULNESS VS. HYPE

Today's security tools are growing increasingly innovative, but innovation does not always correlate with success. "The best technology in the world for the wrong use case is the wrong technology," states Polly.

Before investing in a new security technology, security and facility teams need to come together and identify the problems they are actually trying to solve and whether they already have the tools to solve them. With security budgets increasingly constrained, those looking to adopt new technologies need to justify their expenditures with measurable ROI.

"Security has always been seen as a cost center," explains Stockdale. "But today, it is a driver of efficiency, sustainability, and even revenue."

Security technology can drive ROI through predictive maintenance, energy efficiency, and labor cost savings via automation. By branching away from utilizing security systems solely for security purposes, organizations can elevate the customer experience and streamline operations. "One piece of technology can create ROI in two places, which is the kind of win executives want to see," Polly says.

Another measure of ROI from security systems is business intelligence. In integrated security systems—especially video surveillance and access control—every camera becomes an IoT sensor that can capture not only threat actors and incidents but also crowd flow and behavior. These capabilities can be used to optimize building layouts, improve crowd flow in densely populated areas, and reduce entry bottlenecking. Data can also be shared with HR and marketing teams to provide actionable insights.

"Business intelligence from security tech is the fastest way to get a seat at the executive table," says Polly. "It shows you're driving value, not just guarding doors."

FUTURE-PROOFING YOUR TECHNOLOGY INVESTMENTS

When it comes to choosing security solutions that go the distance, Polly and Stockdale recommend flexible, modular systems paired with open platforms or standards, like ONVIF or BACnet. However, organizations need to be mindful of the way they utilize and support their new technology purchases, even after the transaction is done.

"Once you buy these systems, you own them," Polly says. "You'd better know how to support them—or they'll own you."

Strong manufacturer and dealer support is crucial to ensuring the longevity of your new system. Even if a technology is performing well today, Stockdale emphasizes, it may become a liability later on if support response is slow or proper documentation is poor. Polly advocates for direct manufacturer certification so that end users can troubleshoot without an integrator. "Open platforms, regular updates, and transparent support—that's how you build systems that last," concludes Stockdale.

Register to listen to the full webinar here: **www.securityinfowatch.com/55278988**

Samantha Schober is associate editor of **SecurityInfoWatch.com**.

WEBINAR PANEL

John Polly,
Chief Solutions Officer at ProTecht Solutions Partners

Jarod Stockdale,
Senior Project Manager & Security Consultant at Faith Group

Breaking Down Silos: How Integrated Security Technologies Are Transforming Facility Protection

Why integration is the industry's most urgent challenge—and its greatest opportunity.

by Leor Elfassy

INTRODUCTION: THE STREETS DON'T CHANGE

In his book, *Only The Paranoid Survive,* Andy Grove, former CEO of Intel Technologies coined the term "strategic inflection point" as a time in the life of a business when its fundamentals are about to change. A strategic inflection doesn't just change the players; it changes the fundamental dynamics of the game itself. On the one hand, strategic inflection points present massive challenges to entrenched incumbents in any industry (consider Nokia's struggles against Apple in the smartphone market). On the other hand, they present incredible opportunities for those who understand them and know how to pivot their products and services to better serve the market of today. Grove's assessment is clear: in the wake of a strategic inflection point, companies must strategically pivot, rethink their assumptions, and innovate—or die.

Like many industries before us, the security industry is at the precipice of its own strategic inflection point, and the winners and losers depend on who best understands the fundamentals of its new reality. As buildings become smarter and more interconnected, the real differentiator will be a deep understanding of integration, what it truly is. Shockingly, while the security industry constantly extols the benefits of integration, there is remarkably little integration actually happening in the industry, and more troubling, even less of an understanding of what it really is, how to achieve it, and why it matters. If you're reading this, whether you're an end-user implementing solutions, a manufacturer designing products, or a service provider putting them together, I hope you leave with a fresh perspective on the immense opportunities that lie ahead for our industry to make our world safer, smarter, and more responsive to the needs of the communities we serve.

Before I begin, it's important to explain how I got here. My journey to the security industry started in the most unlikely place. In 1993, my dad, Gideon Elfassy, founded a company called Sound Specialists, which specialized in installing CD players and volume

controls. In 1999, we encountered a quadriplegic client who could only move his left index finger. He gave the team a mission—a way to give him independence with technology. With a healthy dose of optimism, a penchant for innovation, and a stroke of luck, they built a robotic arm that extended out of his wheelchair and brought the world's first commercially available touch-panel right to his fingertips.

They developed a control system software that enabled him to control everything with the touch of a button. Doors, windows, lights, shades, audio, video, and they even built a tracking system using infrared sensors embedded in the walls of his home that would blip his location on a map for his parents and caretakers to find him in his sprawling 30,000-square-foot home. My dad's mantra and indeed our tagline has always been "technology simplified." We use technology to simplify the spaces around us and help improve people's lives.

> "Integration is transformative. It means building modular, interoperable ecosystems that can evolve as needs change."

While in college, I worked for Tesla, where I learned about how to use various sensing technologies for real-time detection, and when I graduated, I was recruited to an amazing start-up, MuleSoft, which paved the way for modern integration as it exists today by building the first platform that unified API development with a hybrid PaaS and iPaaS solution for both cloud and on-premise integration. It's safe to say that while I didn't know it at the time, integration was woven into every aspect of my career.

THE SECURITY INDUSTRY IS CHANGING

So, what have strategic inflection points looked like in the past? A brief look into Grove's own time helps us see the massive change that took hold in the computing industry from the late 1970s to the 1990s. The early years of the computing industry were dominated by large players such as IBM and Compaq. What marked their reign was a completely vertically integrated supply chain. Everything, from the microchips to the hardware, software, sales, and distribution, was owned by one company (sound familiar?). Implementers, more commonly known in our industry as integrators (though I will get to why this is a misnomer later), were proud to call themselves "IBM shops." Yet by the late 1980s, the market had undergone significant changes. Companies such as Intel and Motorola developed purpose-built chips. IBM, Compaq, and new entrants such as Dell and HP introduced hardware, operating systems like Windows and Mac, created purpose-built environments, and provided developers with the tools to develop industry-specific applications directly targeted at specific consumers. Overnight, the conversations changed from "What can I do with a computer?" to "What can a computer do for me?"

What does this mean to the security industry? Ten years ago, most security systems were installed in a back office and seldom touched for the next decade, until an upgrade became inevitable. Yet today, our buildings are experiencing the same revolution that has impacted computing, mobile phones, and enterprise IT—technology is at the core of delivering initiatives faster, improving stakeholder engagement, and making businesses more flexible and prepared to provide future value. To meet these new expectations, core security platforms must evolve beyond their original functions. They are now being asked to contribute data, drive automation, and support enterprise-wide initiatives like ESG, hybrid work, and AI-driven analytics. That's a tall order for systems built to operate in isolation.

This is why integration is the key to modern operations. Proper integration is transformative. It means building modular, interoperable ecosystems that can evolve as needs change. It means empowering systems to share data, adapt dynamically, and be remotely managed in real time. It's less about "tying systems together" and more about orchestrating them into a cohesive and responsive, intelligent platform.

At first glance, integration may seem of concern only to a small group of developers and software engineers. Still, it should be of concern to anyone who cares about keeping their products competitive and how they interact with information living in the outside world. From banking to food service to retail, and of course, security, customers expect their services to be dynamic, available 24/7, and accessible anywhere. In his book, *First Break IT*, Ross Mason coins the term "Enterprise Darwinism," noting a seismic shift in the changing business dynamics of the digital age. In a world where barriers to entry are low, it is no longer the large that eat the small; it is the fast that eat the slow. In any industry, the ability to quickly connect applications, data, and services is the key to success that differentiates the winners from the losers. His message is clear: if customers don't have access to the information they want and need, when they want it, they will take their business elsewhere.

At 4S Security, all our clients tell us that data has a massive impact on their key initiatives. From ESG to life safety to tenant/employee experiences, understanding their environments is core to helping them achieve their mission and enabling their businesses to achieve their goals. However, resoundingly, we hear clients telling us that their systems do not, and in fact, cannot provide them the data that they need. Worse, they tell us they do not feel that their technology environments are nimble and future-ready for the types of innovations that will be asked of them in the next three to five years.

PREPARING FOR THE FUTURE

Where does this leave us? We understand that the industry is currently undergoing a strategic inflection point, shifting from vertical to horizontal, and we recognize that succeeding in this modern technology stack requires the seamless integration of systems, applications, and data. The question then becomes: how do we achieve this connected environment?

Let's first look at what a traditional electronic security project looks like. A client and consultant will work together to evaluate products, develop a specification, and manage an RFP process. Once an integrator is selected, the work begins, and after one to two years of hard work, "the system," meaning a Frankenstein of parts, manufacturers, and ideas, is complete—it works, but with hiccups. The client, who thought he was buying a Ferrari, was sold a box of all the parts needed to assemble one. After all of it is constructed, he is left to figure out how to drive it all by himself.

What should it look like?

Clients select an open-operating platform to meet their desired needs (e.g., video surveillance, access control, visitor management, etc.). Even better, if the system is cloud-based, data storage is now limitless. They then implement open-source hardware to decouple hardware from software, focusing on finding the best system for their needs. As their needs evolve and change, the system selections they made may no longer be completely applicable or may need to be augmented with new products and services. As this occurs, new integrations are written to create a network of combined systems, in which best-in-breed applications are orchestrated together to form a solution where the whole is greater than the sum of its parts.

USE CASE EXAMPLES

Let me provide you with two real-world examples:
One of our clients, a global organization monitoring over 20 sites in both the United States and Europe, sought to equip its SOC (security operations center) operators with a means to respond to threats in real-time. The 4S team developed software that integrated over 15 unique SIP phone systems into a single interface, enabling them to page various areas of their facilities. This was then integrated with vibrational sensors at the fence line that triggered alarms via the access control system and the video surveillance system for real-time visual verification. The result is that if an intrusion is detected, alarms immediately display video on the correct monitor at the right time. Two-way audio allows operators to interact directly with individuals, and all of this is done through an easy-to-use interface that requires little to no training.

The second example involves a unique challenge for one of the world's most significant buildings. At peak times, thousands of people traverse through the turnstiles and are directed to one of four "sky lobbies," which act as transitional floors to other areas of the building. While the elevators are smart, they don't have a way to know in real-time how many people are standing in the lobbies and sometimes buildups occur that affect wait times and tenants who need to get to their floors. Working with building management, we devised a unique solution that connects existing occupancy detection sensors, initially installed for mustering, to the building's elevator system via a series of APIs. We then wrote software that allows building managers to automatically dispatch elevators based on real-time occupancy in the elevator lobbies. Operators can now view real-time occupancy data, as well as access information on the number of elevator runs, which can be helpful in both occupancy and maintenance analysis.

While the world forges ahead with AI and new frontiers of technology, it is essential to remember that the enabler behind all of this is the successful integration and orchestration of data. To succeed, companies must standardize the extraction of data from core and legacy systems, package this data into reusable assets that developers can use to drive automation and business value, and then expose this data through meaningful interfaces personalized to the users and clients they serve.

We believe that forward-thinking manufacturers are providing the tools to enable the great value that these new technologies offer. However, to take full advantage of them, the industry must move beyond its traditional view of how technologies connect and focus on creating a data-driven approach that drives innovation. In the words of Lee Odess, who understands this best, what's been is behind us; now it's about Today Forward.

Leor Elfassy is a security and building automation innovator who helps property owners leverage the benefits of integrating systems for optimum efficiency, security, and safety. He is the Director of Business Development for 4S Security and Sound Specialists in Chicago, Illinois.

Scan. Detect. Secure.

REDEFINING SECURITY SCREENING WITH THE POWER OF AI

For decades, security screening relied on traditional metal detectors and labor-intensive processes. But evolving threat scenarios demand more.

The Rohde&Schwarz QPS201 redefines security by leveraging AI and deep learning. It detects items of any shape or material with unmatched accuracy, offering faster, more flexible, and seamless screening for evolving security challenges.

Discover how to transform your security processes.

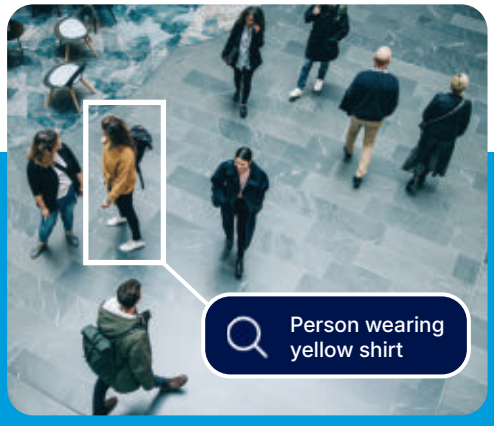
www.rohde-schwarz.com/security-screening

ROHDE&SCHWARZ
Make ideas real

EAGLE EYE NETWORKS

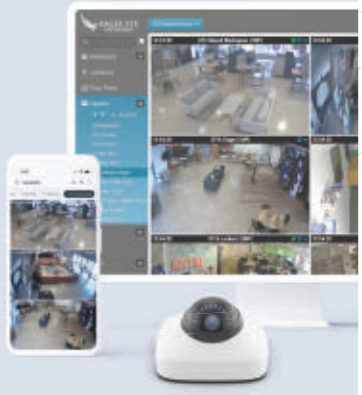
Smart video surveillance is so much more than cameras.

Harness the power of AI to get alerts, trigger actions, increase business insights, and get maximum value from your cameras — without having to replace the ones you have.



Features:

- Artificial intelligence and analytics
- Camera flexibility
- Flexible retention
- Multi-site central management
- Open API for easy integration
- 24/7/365 Customer Support



Scan or click the QR code to learn more

Benefits and Challenges of Integrating Siloed Security Systems

Getting your security technologies to talk to each other isn't just convenient—it helps you avoid missed alerts and respond to incidents quickly.

Here's what you can expect from integration projects.

by Janelle Penny

Can your security systems communicate with each other? If your technologies are still siloed, you may be missing important alerts or responding to incidents later than you should. Coordinating and integrating legacy security systems with new ones into a single, coherent platform lets you avoid these issues and enables real-time monitoring, alerting, and decision-making.

"You're going to have the potential for higher costs because you've got inefficiencies that are in the system" when systems are siloed, explained Sean Ahrens, security market group leader for AEI. "Within the non-integrated system, there is also the potential for a vulnerability to allow a threat to occur. For instance, perhaps we don't have the integration of cameras, so we don't follow up on that one alarm that has always been a 'cry wolf' alarm, and that one time was actually a real occurrence and that leads to an incident."

POTENTIAL PITFALLS DURING INTEGRATIONS

Integrating systems can help avoid these issues, but the integration will naturally come with challenges, especially if you have legacy systems that weren't built to communicate with other technologies, explains Lauris V. Freidenfelds, vice president, security risk consulting, for Telgian Engineering & Consulting.

"You've got to be careful because not all legacy systems will talk to other systems," Freidenfelds said. "You have to have planning and design work done to see how that can actually be accomplished."

One complicating factor is that many manufacturers don't fully support legacy systems anymore and don't test new upgrades on older versions of products, Freidenfelds added. The older the legacy system, the greater the chance that it won't be able to handle something as basic as a software patch, never mind an integration with other disparate systems. "It really is imperative for a security director to plan and budget for upgrades and make sure the versions are maintained and kept current," Freidenfelds added.

BEST PRACTICES FOR INTEGRATING SECURITY SYSTEMS

Integrating security systems starts with bringing on a consultant who is a subject matter expert, Ahrens said. This consultant needs to understand your organization's specific needs in depth.

"Get someone you can partner with that will ask the who, what, when, where, why, and how," Ahrens said. "What types of functionality do you want? How do you want this system to work? What is the goal of this system? Is the intent to integrate this system over a specific time period? Is this a stopgap as you upgrade to the panels that you're planning on using? These are very, very important questions that need to be answered very early on, otherwise you will potentially have costly project outcomes."

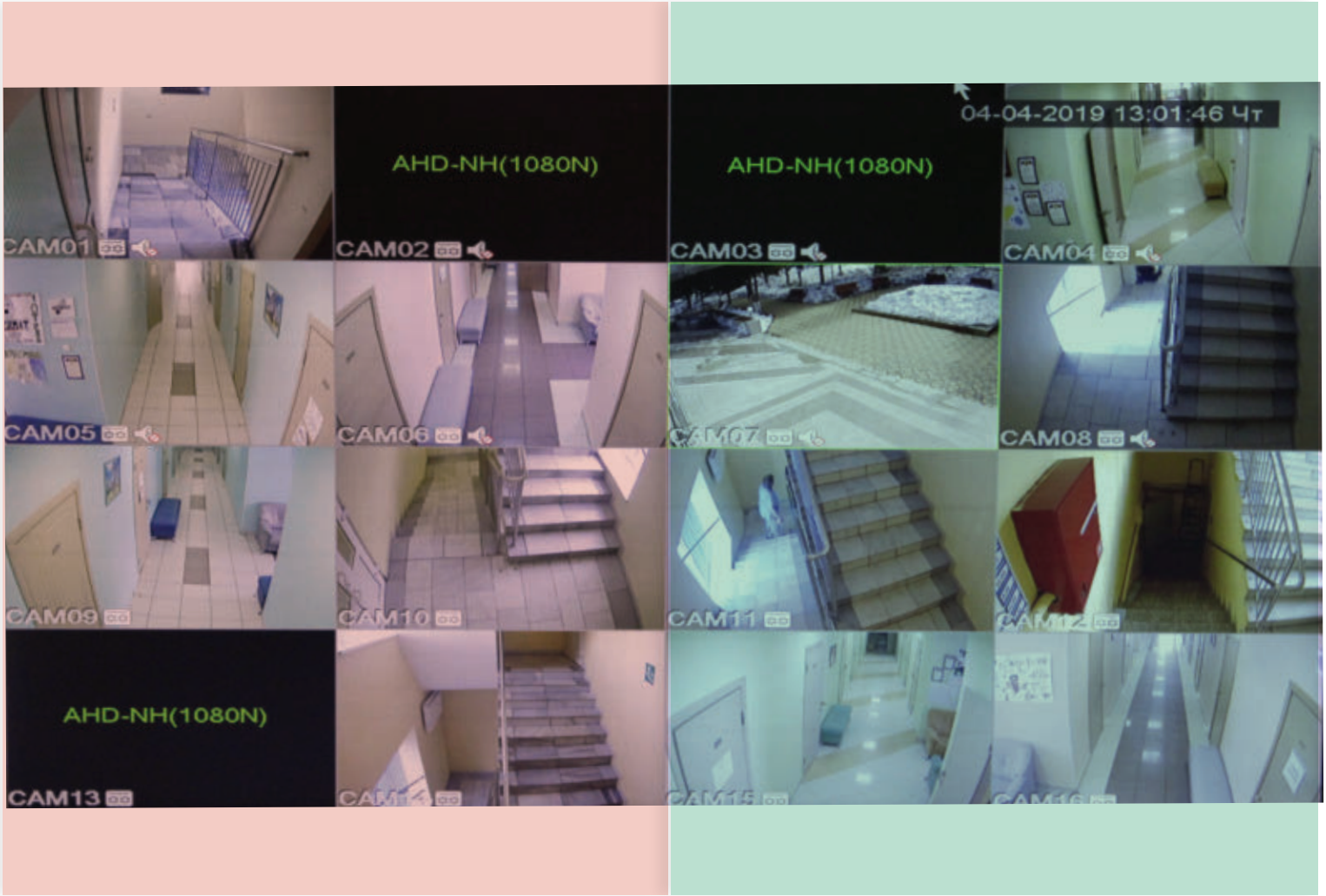
As you bid out the integration project, Freidenfelds recommends looking for consultants who will include ongoing service. Otherwise, you risk ending up with a system that's integrated on day one but may not work in the future when new versions of the components are released.

> "Be careful with the low bid—there is generally a lot missed."

"You really have to invest time, money, and resources to make those systems accomplish everything they're designed to accomplish," Freidenfelds said. "We as consultants who do assessments find that too many times, the systems are installed by contractors and integrators who did the project and didn't do a lot of support for it because they wanted to win the project, so they didn't put too much money into it. You end up with a system that's maybe only 25% effective."

Going with the lowest bid can also mean you've hired an integrator without the right capabilities, Freidenfelds added.

"If you settle in on a manufacturer, make sure the manufacturer can give you recommended integrators that are licensed, have enough support for you, and have the right type of support for you," Freidenfelds said. "Get some information from your designer, consultant, or manufacturer about the contractor and integrator's capabilities. Many of them can hang card readers and things but don't know how to manage a software package, so you've got to make sure to do the background check on those kind of things. Be careful with the low bid—there's generally a lot missed."



ID 153548250 © Roman Gramotenko | Dreamstime.com

Do your different security technologies talk to each other? A smart integration strategy and ongoing service will help ensure everything works together.

As you go through the process of choosing an integrator and consultant, do your homework on what types of systems are out there and their capabilities, Ahrens suggested.

"Come up with your wish list of things you want this system doing in an ideal world," Ahrens said. "The subject matter expert is going to be key to that. Have the people who use the system on a day-to-day basis be part of that discussion—all of that information comes into a functional requirement that the subject matter expert will be able to use to deliver a system that not only the administration wants, but that will be useful to the people/operators using the system too."

A successfully integrated system will deliver an easy-to-navigate platform that your staff can use to keep your building safe, but it will require ongoing work to keep up with new capabilities from manufacturers. A regular review—once a year or at least once every three to five years—will keep your security system up to date and performing the way you need it to.

"It is never complete. It's always a work in progress," Freidenfelds said. "It's not 'We can walk away and it's done.' It's always going to be an evolving concept."

Janelle Penny has been with BUILDINGS since 2010. She is a two-time FOLIO: Eddie award winner who aims to deliver practical, actionable content for building owners and facilities professionals.