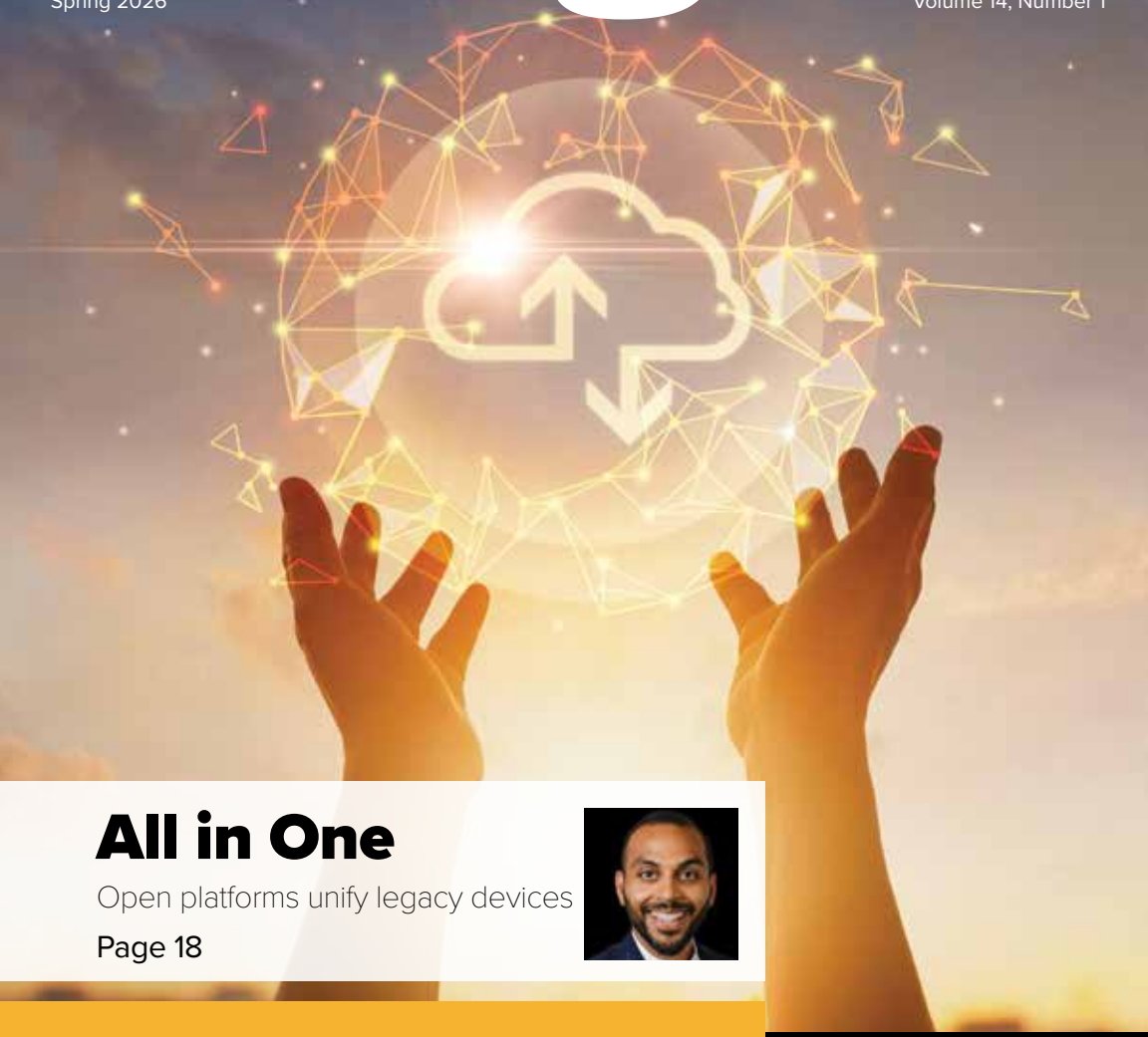
SIA
TECHNOLOGY
Insights
Spring 2026
Volume 14, Number 1



All in One

Open platforms unify legacy devices

Page 18

Information Gathering

Business software now key to integrators' growth

Page 10

Prevent Defense

Proactive AI-powered security can stop incidents

Page 32

Leave and Update

Modernizing security no longer means rip and replace

Page 38

VERIFIED OSDP™ VERIFIED

When you need interoperable, high-security access control solutions, ask for products that bear the OSDP Verified mark.

OSDP Verified means these products have been tested by the Security Industry Association as conforming to one or more profiles of the OSDP standard. For you, that means peace of mind knowing these solutions can communicate securely and seamlessly.

To learn more about OSDP and find a guide to OSDP Verified products,

visit securityindustry.org/OSDP

Security Industry Association
securityindustry.org
SIA

Grow Your Expertise. Grow Your Career.

SIA's Programs for Security Professionals

Security Project Management Training

The SICC: Cybersecurity for Physical Security Pros

Become a Certified Security Project Manager (CSPM)

GrantED: Identify and Obtain Grant Funding

SIAcademy: Online and Live Training

SIA

SECURITY INDUSTRY ASSOCIATION

Explore SIA's Training & Certification Programs

TECHNOLOGY
Insights

Spring 2026 Volume 14, Number 1

SIA Technology Insights is published twice a year, in the spring and fall, by the Security Industry Association in Silver Spring, Md.

All editions are available at no charge at www.securityindustry.org/techinsights.

Questions, comments and article proposals may be submitted to the editor, Ron Hawkins, at rhawkins@securityindustry.org.

Speeding Response When Shots Are Fired

Combining acoustic and infrared detection systems boosts accuracy and effectiveness

Rich Onofrio (ronofrio@shooterdetectionsystems.com) is the Chief Technology Officer at Shooter Detection Systems (www.shooterdetectionsystems.com).

Gun-related violence continues to affect communities across the United States, with 2024 averaging more than one mass shooting per day. As a result, protecting people in outdoor public spaces, such as parking lots, shopping centers, corporate campuses, and stadiums, has become a growing priority for security leaders. This has intensified the need for technologies that can quickly identify threats and support fast, coordinated responses when seconds matter.

Outdoor environments introduce complexities that do not exist in controlled indoor settings. FBI data show that more than half of active shooter incidents in 2023 took place in open areas. Unlike buildings, with access points that can be

monitored and secured, outdoor spaces often involve large, fluid crowds that extend beyond a defined security perimeter. Parking lots, stadium grounds and other sites can change rapidly from vacant to heavily populated, which makes it difficult to manage security and, in the case of a gunfire event, to confirm and determine the precise location of the shots in real time.

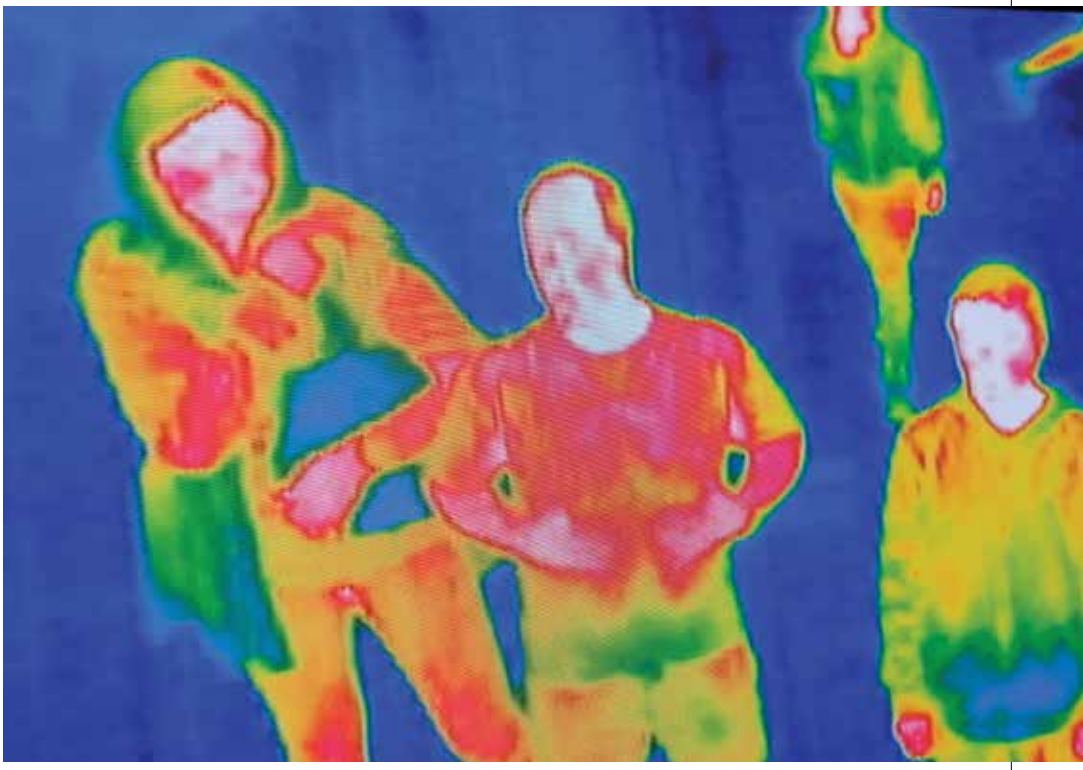
Traditional outdoor gunshot detection solutions have relied heavily on an acoustic-only approach, which is prone to false alerts caused by environmental noise such as fireworks, construction or vehicle backfires. In many cases, these systems also require manual review to confirm a gunshot, slowing response time when immediate action is critical. Today, there are more advanced, dual-factor

> OUTDOOR ENVIRONMENTS INTRODUCE COMPLEXITIES THAT DO NOT EXIST IN CONTROLLED INDOOR SETTINGS.

> WHEN A SHOT IS DETECTED, AN ALERT CAN BE IMMEDIATELY TRANSMITTED TO CENTRAL STATION MONITORING AGENTS WHO CONTACT 911, WHILE ONSITE SECURITY PERSONNEL ARE NOTIFIED SIMULTANEOUSLY.

technologies that utilize acoustic and infrared signals to detect gunshots, addressing traditional systems' limitations by providing higher confidence detection, accurate geolocation, and rapid notification to security teams and first responders.

These dual-factor outdoor gunshot detection sensors are designed to deliver more accurate, actionable intelligence in seconds. When a shot is detected, an alert can be immediately transmitted to central station monitoring agents who contact 911, while onsite security personnel are notified simultaneously. These alerts include critical details such as the precise location of the incident and the exact time it



occurred. This information can dramatically reduce response times and improve outcomes.

During an active shooter event, 911 centers are often overwhelmed with calls, many of which provide incomplete or conflicting information. Delivering accurate gunshot data directly to emergency dispatchers, including details of the sensor location, provides vital clarity during a chaotic and confusing time. This enables first responders to move quickly to the most critical areas, while allowing security teams at campuses, shopping centers and stadiums to restrict access, redirect pedestrians away from danger, and coordinate a more effective response.

Another key advantage of these more advanced outdoor gunshot sensors

DELIVERING ACCURATE GUNSHOT DATA DIRECTLY TO EMERGENCY DISPATCHERS, INCLUDING DETAILS OF THE SENSOR LOCATION, PROVIDES VITAL CLARITY DURING A CHAOTIC AND CONFUSING TIME.

> WHEN GUNFIRE IS DETECTED, NEARBY CAMERAS CAN AUTOMATICALLY SLEW TO THE INCIDENT LOCATION, PROVIDING IMMEDIATE VISUAL CONTEXT AND SUPPORTING LIVE INCIDENT ASSESSMENT.

is their ability to integrate with existing video management systems, access control platforms, and other physical security technologies. When gunfire is detected, nearby cameras can automatically slew to the incident location, providing immediate visual context and supporting live incident assessment. This capability enhances situational awareness and strengthens investigative efforts after the fact.

Integration with access control, mass notification, and emergency management systems further enables organizations to execute lockdowns, evacuations and targeted alerts with speed and precision. Beyond immediate response, outdoor gunshot

detection also supports long-term public safety objectives by capturing valuable forensic data. Information such as geolocation and the number of shots fired can help law enforcement reconstruct events, validate witness statements, and support prosecution. This is particularly valuable in large outdoor areas where physical evidence may be difficult to locate.

As threats continue to evolve, so must the security tools used to address them. Today's more advanced outdoor gunshot detection sensors are not just a technological enhancement, but an essential component of a comprehensive public safety strategy to protect open spaces and the people who visit them. ◀

INFORMATION SUCH AS GEOLOCATION AND THE NUMBER OF SHOTS FIRED CAN HELP LAW ENFORCEMENT RECONSTRUCT EVENTS, VALIDATE WITNESS STATEMENTS, AND SUPPORT PROSECUTION.

The Key to Future Integration Success

Software is now a critical factor in system design

Maureen Carlson (maureen@systemsurveyor.com) is the Co-Founder and President of System Surveyor (www.systemsurveyor.com).

Today's systems integrator faces a unique mix of opportunity and pressure. While demand for system retrofits, modernization projects, and AI-optimized physical security solutions continues to increase, end users also expect faster deployments, clearer documentation, and more proactive lifecycle management than ever before. For many integrators, the most significant day-to-day challenges do not come down to a lack of capable devices or analytics on the market, but rather a lack of streamlined business software to scale operations and deliver consistent high-quality outcomes.

The good news is that the integrator "tech stack" is rapidly evolving. As in other industries undergoing digital transformation, no single software platform can do everything. Instead, best-in-class solutions are emerging that reduce manual data entry, improve visibility across the system lifecycle, and give integrators a more

unified way to manage design, deployment and lifecycle management. Looking ahead, investment in integrated, open software platforms will be essential for integrators seeking to grow their business while meeting increasingly sophisticated customer expectations.

VALUE OF INTEGRATED BUSINESS SOFTWARE

Historically, many integration firms have relied on a patchwork of disconnected tools to run their business. System design lived in one place, customer records in another, project management in spreadsheets, and service documentation in yet another location (often

> BEST-IN-CLASS SOLUTIONS ARE EMERGING THAT REDUCE MANUAL DATA ENTRY, IMPROVE VISIBILITY ACROSS THE SYSTEM LIFECYCLE, AND GIVE INTEGRATORS A MORE UNIFIED WAY TO MANAGE DESIGN, DEPLOYMENT AND LIFECYCLE MANAGEMENT.

> THE GOAL IS NOT TO REPLACE EVERY SYSTEM, BUT TO ENSURE THAT CRITICAL DATA – SUCH AS DEVICE INVENTORIES, SITE DETAILS, AND SYSTEM CONFIGURATIONS – CAN MOVE SMOOTHLY ACROSS WORKFLOWS.

with little or no connection between them). While this approach may have worked when systems were simpler, it introduces friction – not to mention human error – as projects become larger, more complex, and more data-driven.

Open, API-based software architectures are changing this equation. Modern platforms are increasingly designed to share data across applications, reducing duplication and improving consistency. When system design data can flow seamlessly into customer relationship management (CRM), project management, and service tools, integrators spend less time re-entering information and more time delivering value.

This shift toward business application integration is not just about efficiency, it is also about modernization. As integrators adopt AI-enabled technologies, cloud-managed systems, and subscription-based services, their internal processes must evolve as well. Integrated software ecosystems provide a

foundation that supports new business models while reducing operational drag.

AVOIDING APPLICATION SILOS

Most integrators today rely on a mix of tools, such as CRM platforms, inventory management software, enterprise resource planning (ERP) and service ticketing applications. Individually, each tool may perform its function well. Collectively, however, they often create silos that limit visibility and delay decision making.

Optimizing this ecosystem requires a shift in mindset. Rather than selecting tools in isolation, integrators are increasingly evaluating how applications work together. The goal is not to replace every system, but to ensure that critical data – such as device inventories, site details, and system configurations – can move smoothly across workflows.

When design data connects directly to CRM records, sales teams can set clearer expectations with customers. When that same data feeds into ERP and project management systems, ordering and installations become more predictable and less prone to costly surprises. And when service teams have

access to accurate, up-to-date system information, they can respond faster and more effectively in the field.

Platforms that offer native, out-of-the-box integrations allow integrators to modernize incrementally, adding capabilities without extensive custom development. This approach lowers the barrier to adoption and accelerates time to value.

DATA CAPTURE AT SYSTEM DESIGN

As physical security systems grow more complex, customer expectations shift. Today, end users expect their integrators to know exactly what is installed, where it is located, and how it should be maintained over time. Meeting these expectations requires accurate data capture from the very beginning of the system lifecycle.

System design and pre-sales activities, then, represent a critical opportunity, as this is where device selections, deployment needs, and assumptions about performance are established. When this information is captured digitally and structured in a way that can be reused downstream, it becomes a single source of truth for the entire project.

Too often, valuable design data is lost once a sale is complete. Notes from site walks live in personal files, drawings are saved as static PDFs, and critical details never make it into operational systems. The result is a disconnect between what was promised, what was installed, and what is ultimately supported.

Integrated business software helps close this gap. When data captured during design flows into

post-sales workflows, systems integrators gain continuity across the system lifecycle. Installers know exactly what was intended. Service teams understand system context without guesswork. And, most importantly, customers benefit from greater transparency and consistency.

A CONTINUOUS LIFECYCLE

The future of systems integration depends on treating system data as a long-term asset, rather than a one-time deliverable. Design decisions made during site surveys, for example, should inform installation, commissioning, maintenance, and future upgrades. While outdated and over-complicated workflows typically prevent this from happening, integrated software platforms make such continuity possible.

From a business perspective, this approach also unlocks new opportunities. With accurate, up-to-date as-builts and system records, integrators and service providers are

> THE FUTURE OF SYSTEMS INTEGRATION DEPENDS ON TREATING SYSTEM DATA AS A LONG-TERM ASSET, RATHER THAN A ONE-TIME DELIVERABLE.

> AS SYSTEMS BECOME SMARTER AND MORE CONNECTED, THE BUSINESS OF SYSTEMS INTEGRATION MUST EVOLVE ALONGSIDE THE TECHNOLOGY ITSELF.

better positioned to offer lifecycle services, plan refresh cycles, and support evolving customer needs. Instead of reacting to issues as they arise, teams can take a more proactive role.

At the end of the day, customers expect this level of sophistication. Not only do they want to feel confident that their integrator understands the security environment, but they also want to trust that the integrator can guide them through technology changes over time. Integrated business applications and a single point of view about a customer (even when data is moving between applications) help build that confidence and trust.

COLLABORATION ACROSS THE ECOSYSTEM

As with system design and AI performance, successful software integration is not a solo effort. New collaboration opportunities are emerging between integrators, end users and manufacturers, enabled by shared data and connected platforms.

When system information is documented digitally and accessible to authorized stakeholders, conversations become more productive:

- Manufacturers can provide more informed guidance
- Integrators can coordinate more effectively across internal teams and external partners
- End users gain clearer insight into their systems

This collaborative model reduces misalignment and miscommunication and sets more realistic expectations, from start to end. It also supports innovation, as new technologies can be evaluated and adopted with a clear understanding of existing infrastructure.

LOOKING AHEAD

The physical security industry is at an inflection point. As systems become smarter and more connected, the business of systems integration must evolve alongside the technology itself. Integrated, open software platforms provide the foundation needed to scale operations, improve service quality, and meet rising customer expectations.

By prioritizing data capture during the site survey and system design phase, embracing API-driven integrations, and viewing software as a strategic enabler rather than a back-office necessity, integrators can position themselves for short-term success and long-term growth. In the years ahead, the most resilient and competitive integration firms will be those that treat their software ecosystem as thoughtfully as the systems they design for their customers. ◀

Unifying Security Without Overhauling It

Open platforms bring together existing systems while avoiding disruption

Kumar Sokka (kumarsokka@acresecurity.com) is the CEO of Acre Security (www.acresecurity.com).

When business continuity, physical security and cybersecurity operate in silos, gaps are inevitable. Disconnected systems create blind spots and affect response times, adding friction at the exact moment when speed and clarity matter. Converging security and business functions increases efficiency and versatility by reducing duplicative efforts.

Interoperable, standards-based communication creates a single operational view, making event management easier. Fewer interfaces means faster decisions, and a shared view keeps teams aligned, yet many organizations still use fragmented systems. According to a report from Gitnux, only 38 percent of organizations today have physical access control systems that integrate with other platforms, leaving too many teams stitching together answers under pressure.

Existing infrastructure plays a role here, as well. Earlier-generation systems are still effective, but

> DISCONNECTED SYSTEMS CREATE BLIND SPOTS AND AFFECT RESPONSE TIMES, ADDING FRICTION AT THE EXACT MOMENT WHEN SPEED AND CLARITY MATTER.

they are more valuable when they work in tandem with modern solutions on an integrated platform.

ONE ECOSYSTEM TO RULE THEM ALL

Open architecture is the way forward. A system of systems brings data from video, access control, intrusion detection and other components into a single operational view, giving teams a more complete picture of their ecosystem. The idea is to build a bridge between systems, to synchronize people, devices, data and events so that teams can modernize at their own pace while running old and new in parallel.

Connecting systems makes this possible by enabling different technologies to work together without forcing a single-vendor future.

Organizations avoid lock-in and retain the freedom to choose different tools as their needs change. This supports consistent system growth rather than repeated overhauls.

Cloud-enabled platforms also create a shared foundation for collaboration. Security and IT can work from the same data, shifting conversations from "my system versus yours" to "our operation." This shift alone can improve daily workflows.

Using an open platform also preserves prior investments, allowing organizations to extend and improve systems that are performing well instead of discarding them. By design, open architecture supports continuous improvement. It does not force programs

> THE IDEA IS TO BUILD A BRIDGE BETWEEN SYSTEMS, TO SYNCHRONIZE PEOPLE, DEVICES, DATA AND EVENTS SO THAT TEAMS CAN MODERNIZE AT THEIR OWN PACE WHILE RUNNING OLD AND NEW IN PARALLEL.

> SECURITY AND IT CAN WORK FROM THE SAME DATA, SHIFTING CONVERSATIONS FROM 'MY SYSTEM VERSUS YOURS' TO 'OUR OPERATION.'

into rigid technology cycles. Scaling and integration form the engine that pushes security programs forward.

MODERNIZING WITHOUT DISRUPTION

In security, modernization can sound risky. No one wants downtime or operational surprises. The good news is that there is a better way. Organizations can connect earlier-generation systems to newer cloud-based capabilities and create hybrid environments where old and new operate together. This parallel approach reduces downtime and avoids the culture and budget shocks that often come with sweeping change. Teams keep systems running while they introduce new tools in a controlled manner.

When organizations modernize gradually, they can protect previous investments and choose their pace of modernization. This

also eases the human side of change, as teams learn new workflows gradually instead of all at once. Training feels more manageable, and confidence grows naturally.

And, most importantly, security operations continue to run smoothly throughout the process. Modernization supports continuity instead of pausing it.

INVESTING IN UNIFIED SYSTEMS

People want information presented in a simple way. Unified systems deliver this clarity through a single pane of glass – one interface that shows everything simultaneously. Teams can view activity across their entire portfolio without stitching together separate feeds. This visibility supports comprehensive awareness and faster decision making.

When systems work together, security leaders can more easily identify patterns across different vectors and can pair access logs with video footage and alarms to see the full story. This reduces response times and blind spots. As threats grow more sophisticated, end users increasingly value the convenience, scalability and effectiveness that unified platforms provide.

Integration does not require an overhaul. It starts with a choice to connect rather than replace. When leaders consider how their existing tools and investments can work together instead of how quickly they can be swapped out, progress follows. ◀

> MODERNIZATION SUPPORTS CONTINUITY INSTEAD OF PAUSING IT.

The Room Where It Happens

A few key steps can increase security leaders' influence during acquisitions

Chris Martini (chris.martini@zbeta.com) is a Principal Consultant at ZBeta (www,zbeta,com).

Acquisitions are often billed as moments of bold opportunity. For senior executives and boards, these deals are about accelerating growth, unlocking synergies, and strengthening competitive advantage.

But for the teams responsible for making operations run safely and smoothly – including physical security – acquisitions can feel like controlled chaos. Decisions happen without warning, details are opaque, and the ripple effects of choices made in the boardroom cascade down through every layer of the organization.

Too often, physical security is not even in the room where those decisions happen.

When security is treated as an afterthought – a cost center to be rationalized, rather than a strategic enabler – companies expose themselves

to risks that go well beyond access control and surveillance coverage. Overlooked integration challenges can compromise the safety of people and property, slow down facility transitions, inflate budgets, and undermine everyone's confidence in the acquisition itself.

For seasoned physical security leaders, the imperative is clear: Make the program visible, credible and indispensable before and during acquisition conversations.

WHY SECURITY VISIBILITY MATTERS

At first glance, it is not obvious to some why physical security should rank alongside finance, IT and legal in the mergers and acquisitions playbook. But consider what is really at stake:

- Budget accuracy: If no one accounts for systems migration, access credential re-issuance, or security subject matter expert travel during due diligence,

> FOR THE TEAMS RESPONSIBLE FOR MAKING OPERATIONS RUN SAFELY AND SMOOTHLY – INCLUDING PHYSICAL SECURITY – ACQUISITIONS CAN FEEL LIKE CONTROLLED CHAOS.

> FOR SEASONED PHYSICAL SECURITY LEADERS, THE IMPERATIVE IS CLEAR: MAKE YOUR PROGRAM VISIBLE, CREDIBLE AND INDISPENSABLE BEFORE AND DURING ACQUISITION CONVERSATIONS.

financial forecasts will be miscalculated. Underestimating these costs by even a small percentage can throw off larger integration budgets.

- Technology fit: Acquirers frequently inherit access control, video, and monitoring platforms that do not align with their standards. Without early planning, companies risk unsupported infrastructure, avoidable downtime, and duplication of expensive features.
- People and roles: Hasty decisions often bring about security staff redundancies and mismatched responsibilities, resulting in operational gaps and challenges with morale.
- Cultural harmony: Employees at acquired companies can perceive new security measures as heavy-handed

or intrusive, jeopardizing adoption and compliance.

Each of these factors is manageable, but only if companies consider them early on in the acquisition and communicate clearly at the decision-making level.

SECURING A SEAT AT THE TABLE

Physical security leaders should not wait passively for a seat at the M&A table. Instead, they can take practical steps to advocate for it:

1. Identify the M&A committee. This group may go by different names – corporate development team, integration steering group, or even a subcommittee of the board. Pinpoint who leads it and which executives have influence.
2. Make the case for inclusion. Position security not as a compliance hurdle but as a value multiplier. Remind leadership that visibility into risks, costs and integration timelines reduces surprises, accelerates business continuity,

and protects reputation.

3. Bring data, not anecdotes. Prepare a concise playbook that includes current-state inventories of systems and personnel, cost models for typical integration activities, and sample timelines for cutovers. When executives see that security has done its homework, they are more likely to view the function as essential.
4. Leverage allies. Partner with a security consultant, along with facilities, IT, HR and risk management teams who share overlapping interests in safe, seamless operations. Unified advocacy is harder to dismiss than a single voice.

By getting on the M&A committee, security can ensure that their concerns are not raised too late to influence outcomes.

LEADING WITH CREDIBILITY DURING ACQUISITIONS

Visibility is only the first step. Once in the room, security leaders must contribute with authority and clarity. Three practices stand out:

- Translate security into business impact. Executives do not respond to jargon about card readers or VMS licenses; they respond to risk, cost and continuity. Frame every input in terms of:
  - Financial implications, such as “Consolidating platforms will save $X annually, but requires

$Y in upfront integration."

- Operational implications, such as "Delays in credentialing will stall employee onboarding at three newly merged sites."
- Cultural implications, such as "Without a clear change management plan, acquired employees may resist compliance, leading to increased insider risk."

- Provide scenarios, not surprises. Acquisitions move fast, but that should not prevent preparation. Present modeled scenarios – small target vs. large target, regional vs. global integration – and their associated timelines and costs. This

> EXECUTIVES DO NOT RESPOND TO JARGON ABOUT CARD READERS OR VMS LICENSES; THEY RESPOND TO RISK, COST AND CONTINUITY.

> ADVOCATING FOR PEOPLE STRENGTHENS MORALE AND PRESERVES INSTITUTIONAL KNOWLEDGE.

proactive approach demonstrates foresight and earns trust.

- Advocate for people, not just systems. In the scramble to integrate technology, companies often forget the human element. Ensure that acquired security personnel are evaluated fairly, retrained where appropriate, and integrated into the new culture. Advocating for people strengthens morale and preserves institutional knowledge.

VISIBILITY BEYOND A SINGLE DEAL

For some companies, acquisitions are rare, high-stakes events. For others, they are a routine growth engine. In either case, physical security leaders should treat M&As as a recurring test of their

strategic value. To do this, work with a security consultant to:

- Document lessons learned from each acquisition, then institutionalize these lessons in playbooks and checklists.
- Develop clear messaging that explains the security team's mission and impact, so executives understand why the department's presence is essential.
- Commit to realistic timelines for integration work, ensuring leadership sees the discipline and predictability of the security function.

The goal is not just to be consulted during one deal, it is to become permanently visible in the company's growth strategy.

DO NOT BE AN AFTERTHOUGHT

In the popular imagination, the "room where it happens" is a place where power dynamics shift and futures are decided. For physical security leaders, being absent from this room during an acquisition means watching others dictate the future of the program, its people, and the company's entire security posture.

But by proactively seeking visibility – insisting on a voice in acquisition planning, bringing data and credibility to the table, and consistently framing security as a business enabler – leaders can transform physical security from an afterthought into a recognized pillar of successful acquisitions. ◀

Safer Cities, Stronger Economies

Proactive security is now a leadership decision

Kurt Takahashi (ktakahashi@netwatchgroup.com) is the CEO of Netwatch (www.netwatchglobal.ai).

At night, cities become quiet. Parks close their gates. Lights come on. Street activity slows. Public spaces pause until morning. It's a rhythm we often take for granted, but it reflects something important. The expectation that what belongs to the community will still be there tomorrow, intact and ready for use.

When that expectation isn't met, the indicators are visible. A gate bent out of shape. Equipment stolen. Graffiti on bridges and buildings. Over time, these incidents add up. The impact drains budgets, pulls staff away from more crucial tasks, and erodes trust.

City leaders know this isn't theoretical. In 2024, the FBI recorded nearly six million property crimes across the United States. That

reality weighs heavily on municipal decision-makers. According to a National League of Cities report, 94 percent of local officials surveyed rank property crime as a top concern, with a growing share saying it is an urgent matter.

Public spaces usually take the hardest hits. These sites are meant to be open and accessible. They're spread across neighborhoods, and once the lights go down, most of them sit empty. That openness is exactly what makes them valuable during the day, but at night, it can work against them. When vandalism or theft becomes a regular occurrence, and people start to feel uneasy, the use of these areas drops. Local businesses feel it next. And before long, the impact extends well beyond the property line.

> AI HAS CHANGED WHAT SECURITY CAN BE.

For a long time, cities have tried to manage this with tools that tell only part of the story. Cameras that show what happened after the fact. Reports that explain why

> THE DIFFERENCE BETWEEN PREVENTING AND REACTING OFTEN COMES DOWN TO MINUTES OR EVEN SECONDS.

something went wrong once the damage was already done. That can help with accountability, but it doesn't stop a gate from being forced open or a vehicle from disappearing in the middle of the night.

Guard-based models bring their own challenges. Guards play an important role, but covering large, open areas is difficult, and scaling those teams gets expensive fast. Most cities end up stuck choosing between minimal coverage and mounting costs, neither of which delivers the level of confidence residents expect to feel in public spaces.

That's where the approach needs to shift.

AI has changed what security can be. Instead of simply watching and recording, modern systems actively assess what is happening in real time. They help teams spot unusual behavior, recognize when something doesn't belong, and bring issues to the surface early – while there is still an opportunity to step in and stop a problem before it turns into damage.

That timing is everything. The difference between preventing and reacting often comes down to minutes or even seconds. When operators can see what is unfolding and act immediately – whether through live intervention or coordinated response – incidents can often be stopped in time.

And technology can expand coverage without stretching headcount. Many cities look to bring video, analytics and platforms that support

greater situational intelligence together in one place. The data derived from these combined systems can be highly valuable for security operations. First responders arrive on scene more informed, resources can be deployed more efficiently, and a city gains visibility across locations that would otherwise go unwatched overnight.

The impact of this kind of approach goes well beyond security alone. When people feel at ease in public spaces, they spend more time there. When businesses believe an area is well cared for, they are more willing to invest. Research has shown that fear and disorder hold communities back. Stability, on the other hand, creates conditions for growth.

The city of Pico Rivera, Calif., provides an excellent case study.

Located in southeastern Los Angeles County, Pico Rivera was dealing

> TECHNOLOGY CAN EXPAND COVERAGE WITHOUT STRETCHING HEADCOUNT.

> LEADERS CAN KEEP TREATING PROPERTY CRIME AS AN UNAVOIDABLE EXPENSE OR THEY CAN CHOOSE TO INVEST IN TOOLS THAT IDENTIFY THREATS MORE QUICKLY AND BETTER SAFEGUARD COMMUNITY INVESTMENTS. TECHNOLOGY OPENS THE DOOR TO THAT SECOND OPTION.

with repeated theft and vandalism incidents at its municipal golf course. Golf carts and other high-value items were being targeted after hours. Traditional guard services were costly, and visibility across the property was limited once the sun went down. City leaders reached a familiar crossroads: Continue paying for a system that was not delivering results, or step back and rethink the strategy entirely.

They chose to rethink everything.

By implementing an AI-powered video monitoring solution, the city gained consistent, after-hours awareness across the entire course. When suspicious activity was detected, live voice interventions made it clear that the property was no longer an easy target. The dynamic changed and incidents dropped.

"At a time when economic pressure can create opportunities for crime, integrating technology with traditional

law enforcement has proven to be the right move," Pico Rivera City Manager Steve Carmona said. "This approach allows us to protect public assets responsibly while setting an example for other cities facing similar challenges."

The financial side of the equation mattered just as much. By stepping away from a reactive, guard-heavy approach, the city reduced annual security costs by $243,000 without giving up protection. That's more than a line item of savings; it's a sign of smarter decision making.

At its core, proactive security represents a shift in how cities approach an issue. Leaders can keep treating property crime as an unavoidable expense or they can choose to invest in tools that identify threats more quickly and better safeguard community investments. Technology opens the door to that second option.

When cities take ownership of security outcomes, the difference is tangible. Businesses thrive and residents feel more at ease in shared spaces.

That's how cities become safer. That's how local economies grow. And that's what forward-looking leadership looks like. ◀

From Legacy Systems to Modern Functionality

A cloud-managed approach can make upgrades more gradual and manageable

Brian Lohse (blohse@alarm.com) is the General Manager of Alarm.com (www.alarm.com).

Security integrators are entering a pivotal upgrade cycle that represents far more than routine system refreshes. Across commercial security, customers are looking to modernize legacy intrusion, video, access control, and life safety systems by moving toward unified cloud-managed platforms. The opportunity for integrators is significant. Unlike past transitions that required costly rip-and-replace projects, today's cloud platforms can often incorporate and extend much of the hardware customers already own. This shift removes one of the biggest historical barriers to upgrades and

opens the door to a more service-driven growth model.

For decades, integration businesses were built around selling and installing new hardware. Today, value is increasingly created by delivering high-impact services on top of existing infrastructure, including remote management, unified workflows, analytics, and ongoing optimization. This evolution allows customers to modernize faster and more affordably, while giving integrators a chance to move from transactional installation projects to recurring, consultative relationships. The challenge is no longer

THIS EVOLUTION ALLOWS CUSTOMERS TO MODERNIZE FASTER AND MORE AFFORDABLY, WHILE GIVING INTEGRATORS A CHANCE TO MOVE FROM TRANSACTIONAL INSTALLATION PROJECTS TO RECURRING, CONSULTATIVE RELATIONSHIPS.

convincing customers to replace everything at once, but, rather, helping them to begin the upgrade now then guiding them through an efficient, phased migration. This provides benefits to both the customer and integrator.

LEGACY UPGRADE CHALLENGES

Customers often worry that upgrades will introduce downtime, retraining burdens, or new potential points of failure. As a result, integrators routinely walk into environments where hardware still works "well enough," but software and workflows feel stuck in the past, and ownership of systems is split across IT, facilities, operations and security. When the politics of change are as real as the technology, modernization must respect what is already there.

In addition, disparate systems rarely communicate with one another in a meaningful way. Fragmentation between technologies slows investigations

because operators bounce between logins and workflows. For integrators, these silos multiply service complexity and can raise long-term support costs to maintain multiple generations of equipment and software.

CLOUD-MANAGED UNIFICATION BENEFITS

Cloud-managed security platforms offer integrators a structured answer to these challenges. Instead of requiring a fresh infrastructure build, modern cloud solutions can often overlay existing systems and provide a central operating layer that gradually absorbs legacy components.

A cloud platform provides a single operational layer across multi-system environments, allowing

> WHEN THE POLITICS OF CHANGE ARE AS REAL AS THE TECHNOLOGY, MODERNIZATION MUST RESPECT WHAT IS ALREADY THERE.

> LEGACY INTRUSION PANELS ARE A COMMON FIRST STEP BECAUSE THEY ARE OFTEN DEPENDABLE EVEN IF THEY ARE STUCK ON OUTDATED COMMUNICATIONS OR CLUNKY INTERFACES.

users to monitor and investigate events through one interface. When intrusion alarms, door events, and video clips are presented together, operators can move faster and more confidently. Administrative functions also become simpler because user management, site hierarchies, permissions, and system rules can be handled centrally rather than through multiple disconnected tools.

Remote access is another major functionality that customers now expect by default. Cloud management enables browser-based and mobile control, reduces dependence on local workstations, and makes it easier to maintain consistent policies across sites. For integrators,

remote administration and diagnostics lower support friction, reduce truck rolls, and allow updates or configuration changes to be deployed quickly.

Finally, one of the most important benefits for legacy upgrades is hardware flexibility. Cloud unification allows a mix-and-match approach that supports a phased replacement strategy. Customers can keep certain devices, replace others as budgets allow, and add new capabilities without redesigning the system from the ground up. This allows integrators to sell modernization as a journey rather than a cliff, one that begins with connecting what already exists and evolves into a fully modern architecture over time.

THE PATH TO HYBRID MIGRATION

With most upgrade projects, integrators start by connecting what the customer already trusts. Legacy intrusion panels are a common first step

> FIRE AND LIFE SAFETY SYSTEMS HAVE TRADITIONALLY STOOD APART, BUT CLOUD COMMUNICATORS NOW MAKE IT POSSIBLE TO BRING PANEL EVENTS INTO THE SAME OPERATIONAL LAYER WITHOUT ALTERING THE CORE FIRE SYSTEM.

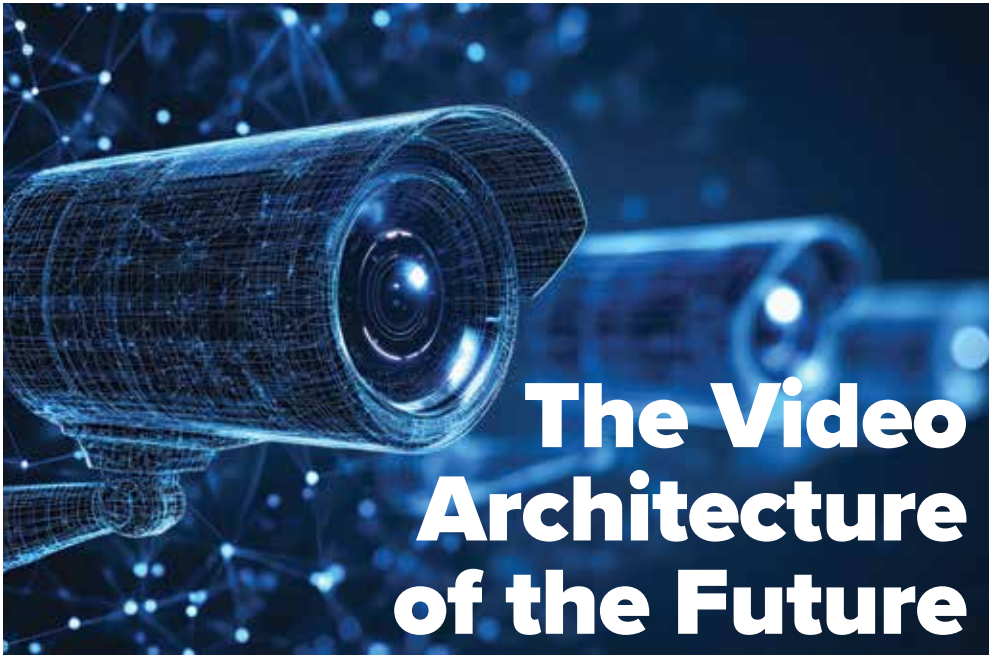
because they are often dependable even if they are stuck on outdated communications or clunky interfaces. With a bridge or universal communicator, these panels can be brought into a cloud-managed layer, giving customers remote control, clearer status, smarter alerts, and a path off phone lines without forcing a full rip-and-replace.

Video is usually the most sensitive part of modernization because cameras represent a big investment and are rarely uniform across a site or multiple locations. Many cloud platforms now support a wide range of third-party models, and retrofit gateways can often pull older cameras into the new environment. This allows integrators to preserve

existing placements while improving the day-to-day experience through unified viewing, faster search, multi-site management, and modern analytics.

Access control follows a similar logic. Customers often delay upgrades because they expect expensive door hardware replacement, but many controller families can be migrated through firmware updates or cloud gateways. Once connected, access policies, credentials and alerts can be centralized across locations, and the real value shows up when access events and video live together in one workflow, cutting investigation time significantly.

Finally, fire and life safety systems have traditionally stood apart, but cloud communicators now make it possible to bring panel events into the same operational layer without altering the core fire system. This adds visibility, automated notification, and faster escalation, rounding out a unified approach that brings security and life safety together. ◀



The Video Architecture of the Future

Edge-to-cloud systems leverage the strengths of both components

For decades, video surveillance followed a familiar blueprint: cameras at the edge, recorders tucked into network closets, and servers humming away in back rooms. It worked well for a time, but it was built for an era when cameras were passive sensors and infrastructure evolved slowly.

That world has changed. Processing power at the edge has accelerated dramatically, networks now expect real-time responsiveness, and cloud platforms have matured into full orchestration layers rather than simple storage destinations. Traditional architectures can no longer keep pace. The next generation of video surveillance requires purpose-built, edge-to-cloud systems engineered to distribute intelligence intelligently, scale predictably, and evolve continuously.

SURVEILLANCE ARCHITECTURE AT A TURNING POINT

Surveillance architecture has always evolved alongside compute capability. Early CCTV centralized everything. The move to network video recorders pushed storage and processing

Jon Marsh (jmarsh@oncam.net) is the Chief Technology Officer at Oncam (www.oncam.net).

closer to the edge, but still tied systems to fixed, site-bound infrastructure.

Today's shift is different because it is driven by convergence. Modern chipsets deliver significant compute inside the camera. Open standards have strengthened interoperability across devices and platforms. Cloud environments have proven themselves as reliable, secure, high-performance control planes for orchestration, analytics aggregation, and lifecycle management.

This convergence enables a distributed model: intelligence where video is captured, orchestration where systems are managed, and storage optimized across edge and cloud based on policy, bandwidth and regulatory constraints. Rather than replacing one centralized system with another, edge-to-cloud architectures rebalance responsibility across the stack.

> ADVANCES IN CHIPSET ENGINEERING HAVE TRANSFORMED MODERN SURVEILLANCE DEVICES FROM SIMPLE CAPTURE ENDPOINTS INTO EMBEDDED COMPUTING PLATFORMS.

ENGINEERING THE MODERN EDGE

At the center of this shift is the camera. Advances in chipset engineering have transformed modern

surveillance devices from simple capture endpoints into embedded computing platforms. Built on sophisticated system-on-chip architectures, today's cameras can run multiple workloads simultaneously.

Leading cameras now perform real-time video encoding, wide dynamic range processing, onboard analytics, health diagnostics, and metadata generation directly on-device. These innovations reduce latency and minimize unnecessary backhaul, all while allowing systems to react locally even when connectivity is degraded.

From an engineering perspective, this requires careful resource management. AI-ready hardware must balance compute, memory and power consumption while operating reliably in challenging environments. Thermal design becomes critical as workloads increase, particularly for devices expected to remain in service for seven to 10 years. The result is a more resilient edge layer that can support evolving analytics models over time, reduce dependency on centralized infrastructure, and adapt to new use cases without wholesale replacement.

CONVERGENCE IN THE CLOUD

As intelligence moves closer to the camera, complexity moves away

from the deployment site. Cloud platforms now serve as the control plane for modern video systems.

In leading edge-to-cloud architectures, the cloud is responsible for provisioning, configuration management, credentialing, firmware updates, and system health monitoring. For organizations managing dozens or hundreds of sites, this centralized orchestration replaces fragmented NVR and server ecosystems with a consistent operational model.

A critical architectural consideration here is metadata-first design. By extracting and structuring metadata at the edge and aggregating it centrally, systems enable fast search, event correlation, and long-term analytics without requiring constant access to raw video. This approach supports both real-time triage and deep learning over historical datasets as models improve.

Importantly, this does not require all video to be streamed continuously to the cloud. Instead, cloud platforms coordinate what is processed, stored,

synchronized or analyzed based on both policy and context.

FLEXIBLE, RESILIENT STORAGE ARCHITECTURES

Storage has traditionally been one of the most rigid components of surveillance systems. By embracing edge-to-cloud architectures, end users are better equipped to balance resilience, cost and accessibility.

At the edge, local storage – often SD-based – provides immediate

> A CRITICAL ARCHITECTURAL CONSIDERATION HERE IS METADATA-FIRST DESIGN.

> CLOUD-ORCHESTRATED PLATFORMS ENABLE REMOTE COMMISSIONING, DIAGNOSTICS AND UPDATES, REDUCING THE NEED FOR ONSITE INTERVENTION.

recording continuity and fast access to intelligent insights. In the cloud, retention policies can be applied selectively based on event importance, regulatory requirements, or operational needs. Intelligent synchronization ensures that video recorded during network disruptions is uploaded once connectivity is restored, without manual intervention.

This hybrid approach offers several technical advantages:

- Retention can be optimized without oversizing local infrastructure
- Compliance requirements can be addressed without duplicating systems
- Uptime improves in environments where network stability cannot be guaranteed

From a systems engineering standpoint, hybrid storage architecture unlocks a policy-driven service rather than a fixed constraint, for end users and integrators alike.

IMPLICATIONS FOR INTEGRATORS

For integrators, edge-to-cloud systems fundamentally reshape how deployments are designed, delivered and supported. Cloud-orchestrated platforms enable remote commissioning, diagnostics and updates, reducing the need for onsite intervention. Over time, this supports more sustainable service models built around ongoing system performance

rather than one-time installations.

Open architectures play a critical role here. Interoperability protects customer investment and allows systems to evolve as requirements change. Rather than forcing rip-and-replace cycles, open systems enable incremental upgrades across cameras, analytics, storage and management layers.

For end users, the benefits are operational. While distributed intelligence improves responsiveness, centralized management simplifies administration, and lifecycle upgrades become predictable rather than disruptive. The result is a system that maximizes budget efficiency while maintaining flexibility as technology advances.

A BLUEPRINT FOR THE NEXT DECADE

The future of video surveillance will be defined by distributed intelligence, cloud orchestration, and open ecosystems. Edge-to-cloud architectures show how a unified design can support real-time analytics,

scalable deployments, and flexible storage without adding unnecessary complexity.

As the industry evolves, the most successful systems will be those engineered for interoperability, resilience and continuous innovation – systems built to align with the realities of modern infrastructure and long-term operational demands. ◀

RATHER THAN FORCING RIP-AND-REPLACE CYCLES, OPEN SYSTEMS ENABLE INCREMENTAL UPGRADES ACROSS CAMERAS, ANALYTICS, STORAGE AND MANAGEMENT LAYERS.

Ensuring that Seeing Is Believing

Built-in authentication is needed to differentiate real video from AI

Jason Crawforth (jason@swear.com) is the CEO of SWEAR (www.swear.com).

A video goes viral. A screenshot sparks conversation. An audio file causes rumors to spread. A single frame steers everything from a boardroom decision to a jury's vote.

The world now runs on digital media, but there's a risk – the internet now manufactures "proof" on demand. Deepfakes and AI-generated forgeries are changing our perception of reality.

The reach of AI-manipulated media is expanding rapidly, and security teams are in the blast radius. According to a study from Graphite, within a year of the launch of ChatGPT, AI-generated articles accounted for 39 percent of all articles published online. And with AI-powered audio and video tools widely available, it's safe to say that Pandora's box has now been opened.

SECURITY IN THE AGE OF AI

Security feels the pressure from AI-generated content more than most other sectors because it sits so close to real-world consequences. The security world protects people and property on a widespread scale, and its systems generate mountains of digital media that shape criminal investigations, legal proceedings, and news media. Video surveillance footage, in particular, is increasingly valuable. It can clear a suspect, confirm an alibi, prove a break-in, or settle a liability claim. If AI can rewrite that evidence convincingly, it won't just cause confusion, it will decide outcomes.

> MANY SECURITY COMPANIES RUSH TOWARD AI-POWERED TECH, BUT FEW ARE PREPARED TO DEFEND AGAINST IT.

Many security companies rush toward AI-powered tech, but few are prepared to defend against it. And online troublemakers are gaining better tools to replace authentic security system content with fake images, audio and video

> THE INDUSTRY NEEDS TO CHANGE ITS MINDSET FROM DETECTING MANIPULATION TO *PREVENTING* MANIPULATION.

that appear convincing. When the tools that create truth and the tools that fabricate "truth" both improve at the same time, action is clearly needed.

DUAL RESPONSIBILITIES

Modern security technologies are now expected to serve two distinct purposes. First, they capture and analyze data to help prevent incidents, enable rapid response, and support effective investigations. At the same time, that data must be preserved in a way that ensures its authenticity, so it can withstand scrutiny from lawyers, regulators, insurers, journalists, and even skeptical juries.

These responsibilities overlap, but they don't solve each other. Forensic technologies can help uncover tampering after

footage is captured, but oftentimes, they are not fast enough. Deepfake techniques are moving quickly, and while investigators work under real-world restrictions – tight timelines, limited budgets, and public scrutiny – bad actors are far less constrained. They don't need everything to go perfectly. Rather, they count on confusion.

PROTECTING THE SOURCE

The industry needs to change its mindset from detecting manipulation to *preventing* it. This shift begins at the point of capture. Authentication technology can embed in each frame of video a cryptographic fingerprint, tying its identity to a chain of custody that cannot be rewritten.

Blockchain fits well here as a practical ledger that preserves custody records against manipulation. By storing footage on a blockchain-based ledger, security teams can provide their video data with proof of authenticity that confirms where footage comes from, where it has

The Global Cyber Alliance reports that, since AI tools became available to the public, incidents of deepfake fraud have increased 1,740% in North America, 1,530% in Asia-Pacific, and 780% in Europe.

> PROVING AUTHENTICITY BUILDS CONFIDENCE AMONG STAKEHOLDERS, PARTNERS AND REGULATORS AND CREATES CONSISTENCY IN HOW INCIDENTS ARE REVIEWED AND RESOLVED.

been, and who has seen it.

This approach also creates a clear chain of custody. Teams can track handoffs through every transfer, and each step leaves a trail that can be audited.

In public safety environments, law enforcement relies heavily on video data for investigations and legal proceedings. Authentication ensures that footage can hold up in court. For security teams protecting critical infrastructure, the ability to verify incidents captured on camera helps ensure compliance with standards and reduces liability. Generally speaking, in any application or market, trusted digital evidence reinforces credibility. Proving authenticity builds confidence among

stakeholders, partners and regulators and creates consistency in how incidents are reviewed and resolved.

DEMANDING PROOF

When authenticity is built in from the start, rather than added later, trust in digital records has a fighting chance in a world that is increasingly skeptical.

This responsibility doesn't belong to one group alone. Builders, buyers and policymakers all have a role to play in advocating for systems that value truth as much as outcomes. Security teams need to ask questions about how digital content can prove where it came from and how it has been handled, and they should support standards that ensure transparency. In a world where almost anything can be fabricated, the real advantage lies with those who can show what truly happened. ◀

> WHEN AUTHENTICITY IS BUILT IN FROM THE START, RATHER THAN ADDED LATER, TRUST IN DIGITAL RECORDS HAS A FIGHTING CHANCE IN A WORLD THAT IS INCREASINGLY SKEPTICAL.

Mitigating the Silo Vulnerability

The GRC framework brings physical security and cybersecurity together

Governance, risk and compliance (GRC) provide an integrated framework for managing security programs across both physical and cyber domains. This high-level approach ensures that security investments align strategically with business objectives, risks are systematically identified and mitigated, and regulatory requirements are consistently met across an organization.

In today's interconnected environment, the traditional separation between physical security and cybersecurity creates vulnerabilities. GRC bridges this gap by establishing a unified framework that recognizes the interdependencies between these domains. When a physical breach occurs, such as an unauthorized person gaining access to a server room, it can turn into a cyber incident. Similarly, cyberattacks may require physical responses, such as facility lockdowns or evidence preservation.

The power of GRC lies in its ability to transform security from a collection of disconnected technical activities into a coordinated, risk-based business function. Rather than treating physical security and cybersecurity as separate silos with different policies, tools and teams, GRC creates a common language and shared processes that enable holistic security management.

The SIA Utilities Advisory Board (www.securityindustry.org/committee/utilities-advisory-board) brings together SIA members and other experts to address compliance and technology topics of interest to professionals managing security at utility facilities.

For practitioners, this means moving beyond compliance paperwork to create an operational framework that makes security measurable, defensible and effective. Organizations that successfully implement integrated GRC gain comprehensive visibility into their risk landscape, optimize resource allocation, and build resilience against evolving threats that span both physical and digital realms.

> WHEN A PHYSICAL BREACH OCCURS, SUCH AS AN UNAUTHORIZED PERSON GAINING ACCESS TO A SERVER ROOM, IT CAN TURN INTO A CYBER INCIDENT. SIMILARLY, CYBERATTACKS MAY REQUIRE PHYSICAL RESPONSES, SUCH AS FACILITY LOCKDOWNS OR EVIDENCE PRESERVATION.

THE THREE PILLARS OF GRC

The GRC framework rests on three fundamental pillars that combine to create a comprehensive security program. Each pillar addresses critical aspects of security management while supporting the others to form an integrated whole.

1. *Governance*: Establishes policies, standards and

> RATHER THAN RECEIVING SEPARATE REPORTS ON PHYSICAL AND CYBER THREATS, DECISION MAKERS SEE AN INTEGRATED RISK PICTURE THAT REVEALS INTERDEPENDENCIES AND ENABLES STRATEGIC RESOURCE ALLOCATION. THIS HOLISTIC VIEW SUPPORTS BETTER INVESTMENT DECISIONS AND MORE EFFECTIVE APPROACHES TO SECURITY.

organizational structures that define how security is managed; creates clear ownership and accountability across both physical and cyber domains

2. *Risk Management*: Identifies, assesses and mitigates threats across an organization; provides a systematic approach to understanding vulnerabilities and their potential business impact
3. *Compliance*: Adheres to laws, regulations and industry standards; coordinates audit programs and regulatory reporting across physical security and cybersecurity requirements

Organizations that successfully implement integrated GRC programs realize significant advantages across multiple dimensions of security management and business operations.

The efficiency benefits stem from eliminating redundant processes and creating a single framework for security management. Organizations no longer conduct separate physical and cyber audits, maintain duplicate documentation systems, or produce multiple risk reports for different stakeholders. This consolidation reduces the administrative burden

and frees security teams to focus on proactive threat management rather than paperwork.

Enhanced visibility provides executives and security leaders with a comprehensive understanding of organizational risk. Rather than receiving separate reports on physical and cyber threats, decision makers see an integrated risk picture that reveals interdependencies and enables strategic resource allocation. This holistic view supports better investment decisions and more effective approaches to security.

Improved resilience results from coordinated security controls that address threats comprehensively. When physical security and cybersecurity teams work from the same playbook and share information seamlessly, organizations close the gaps that attackers exploit. This coordinated approach ensures that security measures in one domain support and reinforce

protections in the other, creating defense in depth.

STEPS FOR BUILDING A GRC PROGRAM

Implementing an integrated GRC program requires careful planning and systematic execution across five critical areas. Organizations should approach this process as a transformation rather than a fixed state, with continuous refinement and maturation over time.

1. Develop a Unified Security Strategy

Begin by aligning physical security and cybersecurity initiatives with overarching business objectives. Ensure executive leadership understands and supports the integrated approach. Develop a security strategy document that articulates how both domains work together to protect the organization and enable business success. The benefits include streamlined governance processes, reduced administrative overhead, and a cohesive security culture that recognizes the interconnected nature of modern threats.

2. Establish a Common Risk Language

Create consistent terminology and risk scoring methodologies across both domains. Develop a unified risk register that captures physical and cyber threats using the same impact and likelihood scales. This common language enables meaningful comparison and prioritization of risks regardless of their origin.

3. Deploy Integrated Technologies

Leverage platforms that bridge physical and cyber domains, such as physical security information management (PSIM) systems integrated with security information

and event management (SIEM) tools. Ensure that access control systems connect to identity management platforms and that monitoring systems feed into a unified security operations center (SOC). Physical and cyber touchpoints represent both vulnerabilities and opportunities for enhanced protection.

4. Implement Cross-Training Programs

Ensure that physical security teams understand cyber threats and that cybersecurity teams appreciate physical vulnerabilities. Conduct joint training exercises and tabletop scenarios that require coordinated responses. Build a culture where security professionals see themselves as part of a unified team rather than members of separate disciplines.

5. Plan for Continuous Improvement

Schedule regular assessment cycles to evaluate GRC program effectiveness. Conduct lessons learned sessions after incidents and exercises. Track metrics that demonstrate program maturity and identify areas for enhancement. Treat GRC as a living framework that evolves with the organization and threat landscape.

A VITAL OPERATIONAL FRAMEWORK

GRC is not just compliance paperwork; it is an operational

> WHEN PHYSICAL SECURITY AND CYBERSECURITY TEAMS WORK FROM THE SAME PLAYBOOK AND SHARE INFORMATION SEAMLESSLY, ORGANIZATIONS CLOSE THE GAPS THAT ATTACKERS EXPLOIT.

> BUILD A CULTURE WHERE SECURITY PROFESSIONALS SEE THEMSELVES AS PART OF A UNIFIED TEAM RATHER THAN MEMBERS OF SEPARATE DISCIPLINES.

framework that makes security measurable, defensible and effective. When physical security and cybersecurity operate in silos, organizations face vulnerabilities, inefficiencies and increased risk. Integrated GRC ensures that security is a coordinated, risk-based business function rather than a series of disconnected technical activities.

For security practitioners, embracing integrated GRC means moving beyond traditional boundaries and recognizing that modern threats do not respect the artificial divisions between physical and digital domains. A comprehensive GRC program provides the structure, processes and tools needed to manage security holistically, demonstrate value to business leaders, and build organizational resilience. The path forward requires commitment to breaking down silos, investing in integration technologies, and fostering collaboration between traditionally separate teams.

Organizations that successfully implement integrated GRC gain competitive advantage through superior risk management, operational efficiency, and the ability to adapt quickly to emerging threats. The question is not whether to integrate physical security and cybersecurity governance, risk and compliance, but how quickly an organization can make this transformation. ◀

Ready to improve how you manage security projects?

Improve Your Security Project Management Skills with SIA Training and Certification Programs.

SPM
SECURITY**PROJECT**MANAGEMENT

More than just knowing the technology, successful project management involves budgeting, client management, timeline execution and more.

Learn more at securityindustry.org/spm

CSPM®
Certified Security Project Manager

This highly-respected credential can move your career forward and propel your business. The CSPM credential informs clients that you can successfully manage complex,technical security projects.

Learn more at securityindustry.org/cspm

Security Industry Association
securityindustry.org

SICC™ SECURITY INDUSTRY CYBERSECURITY CERTIFICATION

THE CYBERSECURITY CERTIFICATION FOR SECURITY INDUSTRY PROFESSIONALS

Why Earn the SICC?

The only credential focused specifically on cybersecurity for physical security systems

Validate your understanding of essential topics like:
- Infosec principles
- Networking and network security
- Device security
- Software security
- Social engineering

Accelerate your career and build trust with your colleagues, partners and clients

"We will be making the SICC certification part of our essential staff training to ensure everyone in our organization has the skills and knowledge they need to face changing cybersecurity challenges and build innovative, secure solutions for our customers."

– Courtney Gibson, SICC, chief technology officer and chief information security officer, BioConnect

Learn More About the SICC

www.securityindustry.org/sicc

SIA SECURITY INDUSTRY ASSOCIATION

Co-developed with support from

PSA SECURITY NETWORK

security specifiers