

SECURITY MANAGEMENT

Published by ASIS International

September 2025



Tell Me More

Connecting metrics with a human-centric narrative can make security's value proposition harder to refute.

By Sara Mosqueda



Physical security, put to the test.

Evaluate, innovate, and evolve your security program with ZBeta LabZ.

Go beyond the traditional barriers to innovative physical security design. Brainstorm with your industry peers and eliminate the guesswork that comes from implementing untested solutions. Through our investment in LabZ; an advanced testing, research and innovation center, ZBeta offers unprecedented opportunities for the companies we work with to achieve new insights into physical security solutions, methodologies, philosophies, and design.

Secure your tomorrow.

Visit us at **GSX Expo Suite #1277**

zbeta.com/labz





H.264 100 Kb

AV1 60 Kb

REC ●

REC ●

The future of video compression is **here.**

See **AV1** only at **GSX Axis booth #1327**

Discover how AV1 is transforming network video.

AXIS[®]
COMMUNICATIONS

Contents Notable

“That hiring process is a black box. You don’t have a lot of visibility into how that person was vetted.”

Greg Schloemer cautions that third-party hiring firms may be particularly vulnerable to North Korean IT worker schemes. [Page 23](#)

442%

The difference in crime solvability when associated video evidence was present in Hartford, Connecticut.

[Page 19](#)

“Metrics are the switches and dials for security program performance measurement.”

George Campbell shares how to leverage the right measurements to tell a compelling story about security.

[Page 27](#)



“They may think that an armed security person can carry out the exact same duties and exact same responsibilities with the level of force that a police officer or law enforcement officer can, and unfortunately that’s not completely accurate.”

Edward E. “Gene” Sanders outlines the constraints around arming security personnel. [Page 37](#)



3,100

The number of people reportedly arrested in relation to protests on college campuses between April and July 2024.

[Page 50](#)



63%

The percentage of job exits in 2024 that were preventable, driven by career stagnation, work-life balance issues, and management failures. [Page 16](#)



Your partner in security and **beyond.**

Hanwha Vision has the right surveillance solutions to protect your operations and keep your business moving forward, combining 24/7 protection with AI, analytics, and cloud management.

Smarter AI, Sharper Images, Stronger Security.

Go **Beyond** Expectations to the future of surveillance.



BOOTH #2326



Contents Features

SEPTEMBER 2025

EXECUTIVE TEAM

William W. Tenney

chief executive officer

William.Tenney@asisonline.org

Christine M. Peck, CAE

chief global learning officer

Christine.Peck@asisonline.org

Nello Caramat

publisher

Nello.Caramat@asisonline.org



1625 Prince Street
Alexandria, VA 22314
703.519.6200
fax 703.519.6299

MEDIA SALES

Cleo Chitester

account manager

703.518.1459

Cleo.Chitester@asisonline.org



COVER STORY

24 Tell Me More

Connecting metrics with a human-centric narrative can make security's value proposition harder to refute.

By Sara Mosqueda



32

ARMED SECURITY

Frameworks of Support

Armed security officers are trained to respond to threats in seconds, but are they prepared to handle the weight of that responsibility?

By Megan Gates



42

EXTREME HEAT

New Extremes

In some roles, working in high temperatures can be inevitable. But changing temperature ranges can make jobs increasingly dangerous without appropriate mitigation strategies.

By Sara Mosqueda



48

MASS PROTESTS

Meeting Peace with Peace

The October 2023 Hamas attack in Israel and its aftermath sparked a new era of campus free expression and protest. Many institutions, including Saint Louis University, had to grapple with how to respond.

By Melinda Heikkinen



Discover trends shaping the future of security.

Get your copy of the
2026 Global Technology
Outlook Report today.



Contents Departments

EDITORIAL STAFF

Claire Meyer
editor-in-chief
Claire.Meyer@asisonline.org

Megan Gates
senior editor
Megan.Gates@asisonline.org

Sara Mosqueda
associate editor
Sara.Mosqueda@asisonline.org

PRODUCTION & CREATIVE SERVICES STAFF

Tyler Stone
art director
Tyler.Stone@asisonline.org

Keith Schilling
manager, publishing production
Keith.Schilling@asisonline.org

Mariah Bartz
associate art director
Mariah.Bartz@asisonline.org

Iuliia Laguta
graphic designer
Iuliia.Laguta@asisonline.org

SECURITY MANAGEMENT

1625 Prince Street
Alexandria, VA 22314
703.519.6200
fax 703.519.6299

MISSION STATEMENT

Security Management is written primarily for security professionals. It also makes vital security information understandable to a general business audience, helping ASIS International advance security worldwide. Readers receive timely information on emerging security threats and practical solutions, which they can use to protect people, property, and information.

14

NEWS & TRENDS

A Believability Gap

Without clear corroborating evidence, third parties are less likely take corrective action when women make reports of workplace abuse compared to men.

By Claire Meyer



18

CASE STUDY

Solvability Rises with Technology, Talent

Connecticut's Hartford Real-Time Crime Center leverages surveillance, an open VMS, and specialized talent to investigate crimes.

By Claire Meyer



20

CYBERSECURITY

Recruitment Red Flags

North Korean threat actors continue to get hired for remote IT worker positions, posing a persistent problem for corporate security teams.

By Megan Gates



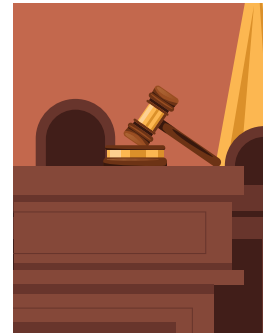
60

LEGAL REPORT

Judicial Decisions

SolarWinds Corp. reached a settlement in principle with the U.S. Securities and Exchange Commission to end litigation concerning a massive 2020 cyberattack.

By Sara Mosqueda



10

CONTRIBUTING AUTHORS

12

EDITOR'S NOTE

Working through periods of change can present opportunities for creative solutions and growth.

56

ASIS NEWS

ASIS International releases three new standards to help practitioners build robust security programs.

58

ASIS GLOBAL BOARD OF DIRECTORS

63

ADVERTISER INDEX

64

INDUSTRY NEWS

A new partnership aims to eliminate integration gaps between video security and mass notification systems.

By Sara Mosqueda

66

INFOGRAPHIC

If true physical-cyber convergence is out of reach, prioritizing partnerships for holistic security instead can pay off.

Contributing Authors



Melinda Heikkinen

ASSOCIATE VICE PRESIDENT, PUBLIC SAFETY

SAINT LOUIS UNIVERSITY

Melinda Heikkinen leads a team of 135 security professionals tasked with protecting the Saint Louis University campus community, including all aspects of security, parking, transportation and cards services, emergency preparedness, and security technology. She has worked in the field of security for more than 25 years in corporate, government, and military areas, both nationally and internationally. A military retiree, Heikkinen served in both the U.S. Marine Corps and the Army National Guard as a flight operations specialist and intelligence analyst.

Heikkinen serves on several boards, including The Ethics Project in Saint Louis and the Grand Center East Community Improvement District, and she previously served as co-chair for StandPoint. She is a member of the ASIS International CSO Center, working on the thought leadership committee. Heikkinen holds master's degrees in organizational leadership and history, as well as a bachelor's degree in aeronautics.

[“Meeting Peace with Peace,” Page 48](#)

Kevin Cassidy

Kevin Cassidy lectures at John Jay College of Criminal Justice in New York City and at Slippery Rock University in Pennsylvania. He is also a member of ASIS International.

[Book Review, Page 15](#)

Ben Rothke, CISSP, CISM, CISA

Ben Rothke, CISSP, CISM, CISA, is a New York City-based senior information security manager with Tapad who has more than 20 years of industry experience in information systems security and privacy.

[Book Review, Page 21](#)



Trust

in the moment

With the right people, advanced technologies, and tailored security solutions, our customers trust us to help protect them in the moments that matter most — backed by an expert local team with a proven record of delivery.

Booth #1627
aus.com



CREATIVITY AND CHANGE

Change is constant. Some changes are positive, others surprising, and a few will completely throw you off your game. How you adapt will determine your ability to succeed and add value to your organization.

Richard Widup, CPP, worked through a major episode of change when his employer—an infant formula manufacturer—was acquired by a fast-moving consumer goods company. This completely changed the culture of the security function. It had previously been a widely accepted support to regulatory compliance and safety, but in the new environment, Widup had to make a business case for every dollar allotted to security, extolling the need for and value of security awareness and risk management protocols to each decision-maker worldwide.

Although this required political savvy from Widup and his team, as well as constant outreach to other executives, it ended



Maybe having to fight for dollars and other resources, maybe that's not a bad thing because now we need to be better at quantifying our value.



up being a net positive because the security function became more adaptable and better aligned with other business functions.

"It was a wake-up call," he says. "We got it—this is the way the business operates. If we want to be successful, if we want to be seen as an enterprise-driven organizational element that adds value to the company at all levels, all times, then we need to adapt."

"We have to understand also that we're not going to win all the battles anymore," he continues. "And maybe having to fight for dollars and other resources, maybe that's not a bad thing because now we need to be better at quantifying our value."

Quantifying the value of security meant making faster and more compelling presentations to stakeholders, listening to and addressing regional leaders' unique needs, and documenting the long-term benefit of security's involvement on those leaders' personal bottom lines as part of a continual value proposition.

This issue of *Security Management* is full of examples of how security professionals adjusted to changing conditions, incorporated requirements from stakeholders, and identified emerging risks. But like Widup found, the solutions are rarely straightforward. They require creativity, conviction, and some convincing metrics.

In "Tell Me More" (page 24) security practitioners explore creative ways to connect business-centric metrics and key performance indicators with more human narratives that tug on heartstrings and loosen purse strings. That includes some unconventional security decisions, such as inviting graffiti artists to participate in crime prevention initiatives. That creativity was worthwhile to a series of convenience stores in Canada, especially since the value of those programs could be measured and communicated effectively.

Want to learn more about managing security through periods of change? Check out the *Security Management* series on the topic, including more of Widup's story, online at asisonline.org/SM-change-management. ■

Claire Meyer
Editor-in-Chief

SECURITY AT RECORD SPEED.



OPENGATE® Groundbreaking Weapons Detection System

- Quickly and automatically screen guests with their backpacks, purses, and bags in transit
- Extremely high throughput with near zero nuisance alarms
- Detects handguns and mass casualty threats, such as high caliber assault weapons and IEDs
- Easy to relocate at 25 pounds and installs in less than 1 minute
- Indoor and Outdoor operations



Our weapons detection and screening systems take the guesswork out of security screening. Incorporating the latest in threat detection technology, CEIA sets the standard for safety, convenience and accuracy.

For more information, contact your CEIA USA representative at security@ceia-usa.com or call us today at **833-224-2342**.



A Believability Gap

Researchers found that in situations without clear corroborating evidence, third parties are less likely to take corrective action when women make reports of workplace abuse compared to men.



By Claire Meyer



Organizations encourage employees to report abusive behavior, whether through tiplines or informal measures like disclosing bad behavior to managers. Some of those methods are less effective than others and can produce gaps in appropriate investigations and responses. But new research demonstrates that it's not just the how of reporting that makes a difference, it's the who.

Researchers from the University of North Carolina at Chapel Hill and the Wharton School at the University of Pennsylvania found that in situations without

Our research suggests that these anonymous reports may be met with skepticism, in part because of low levels of corroboration.

clear corroborating evidence, third parties are less likely to take corrective action when women make reports of workplace abuse compared to men.

Making matters worse, it's relatively common for workplace abuse complaints to lack significant evidence of abuse, says Timothy Kundro, assistant professor at UNC Chapel Hill's Kenan-Flagler Business School. He was the lead author on the research, *Reject or Protect? Corrective Action in Response to Women's vs. Men's Reports of Workplace Abuse*, which was recently published in the research journal *Organizational Science*.

A preliminary study for the research found that 70 percent of workplace abuse reports relied solely on verbal accounts and that most corroborating evidence was rated low on average. This means that manager discretion often played an outsized role in determining if reports were escalated, Kundro tells *Security Management*.

But where does gender bias come in? Kundro says that he and his fellow researchers wanted to study this element of workplace abuse because there are “competing ideas about how a reporter’s gender affects managers’ decisions. Some believe managers will ignore reports made by women because they see them as less credible. Others believe that managers will take these reports particularly seriously because of liability or reputational risk. Both seemed plausible, so we wanted to dig deeper to understand more.”

The researchers used a large government study of more than 2,000 employees from 2016 and noted that women’s reports of abuse were ignored more often than men’s. They then ran several experiments to test their hypothesis, asking participants to evaluate different reports of abuse made using artificial intelligence (AI) audio.

“In one study, people listened to a short, very realistic recording made by AI—either a woman’s voice or a man’s voice—saying the exact same thing about a coworker’s abusive behavior,” Kundro says. “In some cases, participants were given evidence supporting the report; in others, they weren’t given any evidence. When there was no supporting evidence, people who heard the man’s voice took the complaint more seriously than those who heard the woman’s. Specifically, they were more likely to escalate the complaint to the research team. But when evidence was provided, people treated women’s and men’s reports the same.”

But anonymous reports are not the solution, either.

“...Our research suggests that these anonymous reports may be met with skepticism, in part because of low levels of corroboration,” the research report said. “As a result, anonymous reports may be more likely to be ignored. Thus, organizations should consider ways to increase corroboration when reports are made anonymously.”

The researchers also tested different kinds of evidence—written proof from chat logs and eyewitness confirmation.

“Interestingly, both types of evidence had the same effect and eliminated the gender bias that we saw when no evidence was provided,” Kundro says.

In an article for *Harvard Business Review*, the researchers outlined five ways organizations can improve their reporting and investigation processes to reduce potential gender bias.

Separate report evaluators from report receivers. Managers shouldn’t have to decide which reports to act on, the researchers asserted. Allegations of abuse should be forwarded to a centralized team to evaluate misconduct to reduce bias and assumptions in the process.

Standardize how reports are evaluated. “Create a consistent, formal process for assessing all reports of abuse or mis-

conduct,” the researchers wrote. “One effective strategy is to redact identifying information (e.g., name, gender, role) to reduce the influence of identity-based assumptions and eliminate penalties tied to anonymous reporting.”

Commit to following up on every report. Organizations should establish a clear policy that all reports will receive a formalized, documented follow-up. This helps build trust with employees and makes the process more transparent.

Create alternative and protected reporting channels. Employees shouldn’t have to rely solely on their manager to raise concerns, the researchers said. Consider creating both reporting channels like tiplines and proactive outreach like pulse surveys to solicit employee concerns.

Book Review

Common Sense Police Supervision

By Gerald W. Garner. Charles C. Thomas Publisher, LTD; 358 pages; \$54.95.

Gerald Garner’s book, *Common Sense Police Supervision: Practical Tips for the First-Line Leader*, 7th edition, is a well-written and well-organized book that emphasizes the importance of common sense and leadership qualities within any law enforcement agency. Garner has updated and expanded this book by incorporating specific common-sense criteria and guidelines for police supervisors to follow in various situations.

Garner does an excellent job of focusing specifically on police supervision in a multifaceted society, which is much different than corporate America. Garner writes, “This edition will not enable the reader to speak glibly in the latest, pop management catchphrases and buzzwords. What this edition does offer is solid, practical leadership advice developed from the experiences and observations of real police supervisors.”

This 358-page edition contains a preface, introduction, 20 chapters, and an index. Each chapter incorporates ideas

and strategies for the reader to follow and expertly interlaces the previous chapter into the next chapter. Chapters then conclude with a summary and points to remember.

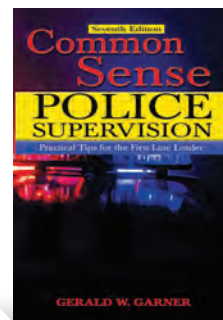
Garner presents his ideas and strategies effectively throughout the book. For example, in chapter 2, readers will appreciate his concepts around psychological preparation and test-taking skills.

He discusses current case law, supervisory principles and boards, and assessment centers, which are important elements for promotion and advancement.

Chapter 14, “The Police Leader’s Role in Community Policing,” can apply to police officers and supervisors. The chapter deals with the importance of diversity and law enforcement in the community.

This is an excellent book that law enforcement, police science, and criminal justice students would benefit from.

Reviewer: Kevin Cassidy lectures at John Jay College of Criminal Justice in New York City and at Slippery Rock University in Pennsylvania. He is also a member of ASIS International.



Support reporters with follow-up tools.

Given the importance of corroborating evidence, organizations can give reporters options to provide additional information later, including about similar events they witnessed.

Even if organizations implement these changes, the human element still reigns supreme. Recent research demonstrates the outsized importance of managers in employee engagement and satisfaction, and their value in misconduct reporting is similarly huge.

“Survey data suggests that people feel more comfortable reporting abuse to their manager rather than using formal organizational reporting systems,” Kundro says. “So, this means that managers need to realize that they’re probably the first line of defense—and their decisions can often determine if reports of abuse are ignored or taken seriously. I think it’s easy for managers to downplay their role here, but our paper suggests that they’re particularly important and impactful.”

Is Turnover Preventable?

Employee turnover is not inevitable; it continues to be driven by preventable reasons that organizations can address, especially career development.

Preventable turnover driven by career stagnation, work-life balance issues, and management failures accounted for 63 percent of all job exits in 2024, according to the Work Institute’s *2025 Retention Report: Employee Retention Truths in Today’s Workplace*. The quit rate—a measure of voluntary turnover—declined to its lowest levels in recent years in 2024, with an average of 3.3 million workers quitting each month. Despite this, around 35 to 40 million employees are likely to quit in 2025.

“Retention is not an accident. It is the result of deliberate choices,” the report said. “High-retention organizations embrace accountability, listen to their workforce, and act decisively to address systemic challenges. As turnover costs rise and workforce mobility persists, employers have a critical choice to either invest in their people or risk falling behind in a competitive labor market.”



The Work Institute conservatively estimated that the financial impact of turnover is 33 percent of an employee’s base pay, with labor shortages and competition for talent amplifying those costs. This means replacing an employee who earns \$50,000 a year could cost the organization \$16,500 or more in 2025. First-year turnover is the most challenging—as much as 40 percent of overall employee turnover occurs within the first year of employment, delivering minimal return on investment for the organization’s recruitment and onboarding costs.

“This makes proactive retention efforts not only a strategic advantage but also a financial necessity,” the report said.

The report analyzed tens of thousands of exit interviews across various industries to assess current workplace dynamics, and it identified a few key findings.

Career Development Over All

People leave their jobs for a wide variety of reasons, but a lack of career growth opportunities, inadequate career progression, or insufficient professional development was cited as the reason for leaving by 18.9 percent of quitters in 2024. This factor showed a slight decline in 2024 compared to previous years, suggesting that some organizations addressed their career growth opportunity issues, but it remained a critical turnover driver, the report said.

Only 14 percent of leaders surveyed for the report strongly agreed that they provide effective career development

opportunities for employees. Significant gaps in career development include:

Limited internal mobility.

Employees cited a lack of visible and accessible internal career opportunities as a major frustration that could push them to leave.

Insufficient professional development. Organizations that lack robust training programs, leadership guidance, and skill-building opportunities can leave employees frustrated about reaching their potential.

Misaligned aspirations and roles. A lack of communication between employees and

their managers about career goals and capabilities creates dissatisfaction and disengagement.

“Employees increasingly prioritize roles that offer clear growth trajectories and meaningful development opportunities,” the report said. “As workforce expectations evolve, the ability to provide these elements is no longer a differentiator but a baseline requirement for retention of the emerging workforce. Failure to address career-related concerns creates a ripple effect in loss of institutional knowledge, increased recruitment costs, and diminished employee engagement among remaining team members.”

Retention is not an accident. It is the result of deliberate choices.

Of people who left their jobs because of career development issues, more than 5 percent left to pursue a different career, nearly 5 percent to get a promotion, 3.5 percent to go back to school, and 2.5 percent for career development.

Managers Really Matter

Gallup’s *State of the Global Workplace 2025 Report* found that engaged managers lead to stronger team engagement and less burnout. Only 27 percent of managers are currently engaged, however, with competing demands, workplace stressors,

and a lack of professional development hitting them hard. For employee retention, this is a big problem.

In 2024, 9.7 percent of employee turnover was directly attributed to management issues, a hike from 7.4 percent in 2022, reflecting the growing strain on managerial effectiveness, the Work Institute report found. Exit interviews consistently cited poor professional behavior, a lack of support, and ineffective communication from managers.

“Recent research indicates managers are asked to take on an ever-expanding array of responsibilities that range from administrative tasks to the implementation of organizational change initiatives,” the report said. “While these responsibilities are often critical, they reduce the time available for managers to build relationships with their teams, provide coaching, and offer meaningful support.”

The Work Institute report recommended that organizations pursue actionable solutions to empower managers and address the root causes of engagement issues, including:

Reduce non-leadership responsibilities. Analyze managers’ workloads and off-load administrative or non-critical tasks.

Provide professionalism and leadership training. This echoed guidance from Gallup, which strongly recommended giving managers the leadership skills they need to feel more comfortable coaching and developing employees.

Analyze span of control. Do managers oversee too many direct reports? Optimize team sizes to ensure employees get individualized attention and support from managers.

Keep Assessments Proactive

The report strongly recommended leveraging stay interviews—like an exit interview but for retention—to get a better picture of employees’ career aspirations, challenges, and concerns.

“Stay interview strategies identify and address potential issues before employees consider external opportunities,” the report said. “Many organizations find external stay interviews a more effective tool to uncover employee career concerns.”

Stay interviews help organizations build a culture of trust and mitigate

emerging turnover risks. Employees are also likely to feel more valued when they see their feedback leads to meaningful changes, the report said. This does require the organization to actually take action, though, and demonstrate responsiveness to employees by openly sharing action plans and communicating how their feedback drove improvements.

Exit interviews are also helpful. “Exit interviews provide invaluable insights into the conditions, behaviors, and decisions that prompt employees to leave,” the report explained. “However, their true value lies in their predictive power. By analyzing trends and recurring themes, organizations can anticipate and mitigate similar risks for the remaining workforce.” ■

MODEL 773 M30 DROP ARM BARRIER

ASTM F2656 Tested — M30/P1 Certified



WE'LL BE
AT GSX!

Look for **Booth #1455**



**BARRIERS
& BOLLARDS**

AMERISTARPERIMETER.COM
866-467-2773

AMERISTAR®

ASSA ABLOY

See us at GSX Booth 1455

Solvability Rises with Technology, Talent

Connecticut's Hartford real-time crime center leverages surveillance, an open VMS, and specialized talent to investigate crimes.



By Claire Meyer



Unsolved shootings fail to provide justice for victims and contribute to a cycle of violence, undermining police efforts to deter gun violence.

Better criminal case solvability means faster investigations, higher apprehensions, reductions in drivers of crime, and greater trust from citizens. In Hartford, Connecticut, technology, data-driven processes, and specialized analysts came together in its police department's Capital City Command Center (C4) Real-Time Crime Center (RTCC) to deliver improved solvability.

The Hartford Police Department founded the C4 in 2015, pulling disparate technology from across the city into a centralized investigative and response function. Now, when police officers are responding to a report of a shooting, analysts are already pulling up surveillance footage, license plate readers, analytics, and other tools to help officers in real-time.

"Police can't use technology while they're driving to a crime," says Sgt. Chris Mastroianni, supervisor of the C4 RTCC and the intelligence division in the Hartford Police Department. "...The last thing you can do is start using cameras and license plate readers while going to the scene. So, our goal here in the center is we're going to do that for them and just give them what they need in real-time."

Now, virtual responders often beat police to the scene, enabling faster evidence-gathering and a more intelligence-led response to incidents. This advance work can lead to greater solvability, Mastroianni says.

Nonfatal shooting cases are notoriously difficult for law enforcement investigators to solve, especially when witnesses and victims are uncooperative.

"Given that a relative minority of shooters in most cities are apprehended for their crimes, it can be difficult to overcome the legal cynicism and fear of retaliation that prevents many victims and witnesses from aiding investigations," wrote Mastroianni and Dr. Lisa Barao, who is now associate director of research at the Crime and Justice Policy Lab at the University of Pennsylvania, in a *Police Quarterly* study. Unsolved shootings fail to provide justice for victims and contribute to a cycle of violence, undermining police efforts to deter gun violence while contributing to individuals' motivations at retribution.

But technology alone isn't an effective crime deterrent without action and process for its usage, Mastroianni says.

“Why would crime go down just because you put a plastic camera on a pole?” he asks. “If you put a fire hydrant on the street, it doesn’t prevent fires and it doesn’t make fires go out faster. You need a process for how that technology is used.”

The C4 RTCC connects approximately 1,400 surveillance cameras across Hartford, integrated with automatic license plate reader (ALPR) technology, gunshot detection, and more. Milestone Systems’ XProtect video management software (VMS) ties disparate systems together through an open architecture, allowing the department to use various technology providers as it scales up and requires customizations, Mastroianni says. Plus, a custom Slack implementation enables analysts to push video, image, and intelligence data and information in real-time directly to officers’ mobile devices.

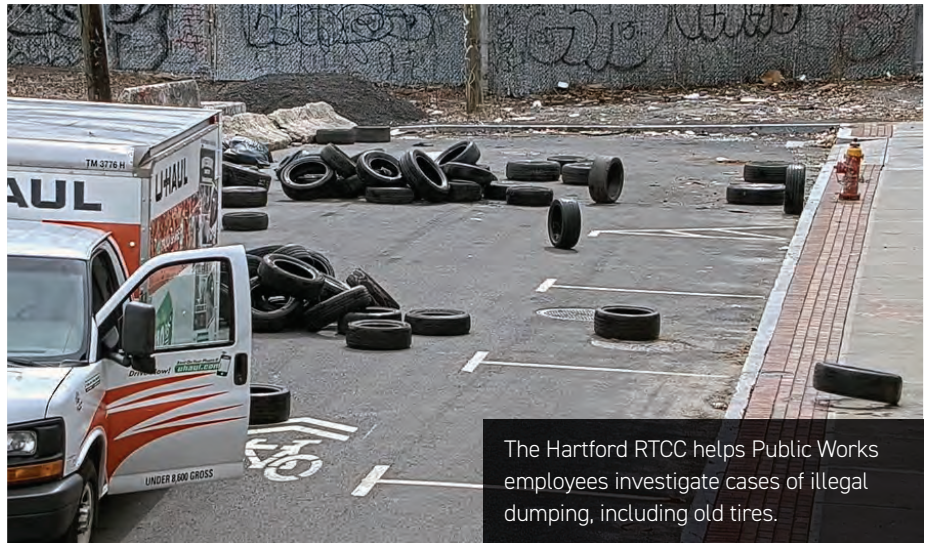
For example, in the event of a robbery at a gas station, RTCC analysts will virtually respond to the scene as police drive to the location. Analysts will capture images of the criminal’s car and push those images to responding officers. If the license plate is recorded, analysts will run the plate number and get the owner’s information and address. These efforts help create solvability.

Even though the technology is valuable, lots of RTCCs and police departments forget about the human element. Well-trained end users are the most important piece in leveraging technology for incident response, he says.

Some police departments use RTCCs as a place to send injured police officers on desk duty, Mastroianni says, cycling them in and out based on their recovery status. But this short-term assignment cannot compete with a specialized, trained analyst’s ability to leverage the technology and assist officers in the field.

“A lot of police departments and agencies just blow money on technology, and they don’t really identify who’s going to use it,” Mastroianni adds. “...It’s important to invest just as much in your humans as in your technology.”

Mastroianni recommends that departments leverage more civilian real-time analysts who can bring specialization to RTCCs, although that can require a culture shift from some police departments that balk at bringing in non-officers.



The Hartford RTCC helps Public Works employees investigate cases of illegal dumping, including old tires.

The C4 function also invests in training staff, especially since the center provides real-time crime assistance, investigative support, and digital forensics for the police department. Some analysts need to specialize in cellphone forensics or other programs, but all of them need training in video surveillance basics and analytics. This enables them to both perform their jobs and be ready to adequately articulate their responsibilities and how surveillance works to a jury, if needed.

The analysts, police officers, and Mastroianni are also primed to articulate the RTCC’s work to other stakeholders across the city and community, which has paid off in surprising ways.

Mastroianni gives RTCC tours to churches, community groups, Boy Scout troops, and news crews—the room is not hidden, and he says that the benefit of promoting C4’s work outweighs the risk.

This openness has helped Mastroianni identify win-win opportunities with other departments. C4 analysts regularly help Public Works employees with illegal dumping investigations, including when someone was purchasing disused boats and then dumping the boats on city streets to cash in on the scrap metal from the trailers. In a 12-month period in 2024 and 2025, the C4 team helped open 33 arrest warrants for illegal dumping through a dual initiative with Public Works.

“We offer to help other entities to get the entire city to buy in that this is a city initiative, not just a police department surveillance center,” Mastroianni says.

By promoting openness and partnerships with C4, Mastroianni has won the loyalty of power company executives, IT department leaders, and his maintenance vendor. But many partners and stakeholders want more solid, long-term data to encourage them to buy in.

Mastroianni partnered with Barao at the University of Pennsylvania to comb through C4’s data on criminal gun homicides and nonfatal injury shootings. They also reviewed the C4 activity tracker, which contains a log of all activities—technologies and programs used, associated case information, and descriptions of analyst actions—related to criminal investigations.

An analysis of case outcomes found that C4 provided investigative support for 86 percent of the 243 investigations. The research found that gun homicide and nonfatal shooting assaults with associated video evidence were 442 percent more likely to be solved than cases without video evidence.

This enabled Mastroianni to successfully argue for more C4 shifts and more personnel, even when the administration in charge of the city changes or budgets tighten.

Often, when visitors see the crime center, it can seem overwhelming with 14 employees and the technology, according to Mastroianni. “They don’t realize that we started in a Tahoe with one intern analyst, and we grew,” he says. “It takes time to piece this all together, but good data is how we continue to grow.” ■

Recruitment Red Flags

North Korean threat actors continue to get hired for remote IT worker positions, including at Fortune 500 companies, posing a persistent problem for corporate security teams.



By Megan Gates



The 2021–2024 scheme compromised the identities of more than 80 people and caused damage and losses of at least \$3 million.

The job market these days is competitive, but personal branding can push a profile to the top of the stack. Just ask North Korean threat actors, who have been using polished LinkedIn profiles to find their next well-paid position.

In June 2025, the U.S. Department of Justice (DOJ) indicted North Korean actors allegedly assisted by individuals in China, Taiwan, the United Arab Emirates, and the United States to successfully obtain employment at more than 100 U.S. companies—including many Fortune 500 firms. The 2021–2024 scheme compromised the identities of more than 80 people and caused damage and losses of at least \$3 million, according to the DOJ.

North Korea began dispatching thousands of skilled IT workers around the world in 2022 to generate revenue for the country's weapons of mass destruction and ballistic missile programs—violations of U.S. and UN sanctions.

The scheme continues to be successful three years later as the threat actors leverage artificial intelligence (AI) tools to create more convincing fake profiles that lead to real job leads.

The FBI and private security partners briefed the security community on the persistent problem at the 2025 RSA Conference (RSAC) in May. The rise of remote work during the COVID-19 pandemic compounded the issue because the North Korean regime realized individuals could get legitimate jobs, at scale, from private companies, says Adam Meyers, senior vice president of threat intelligence at cybersecurity firm CrowdStrike. As of February 2025, CrowdStrike had responded to 304 incidents involving this tactic, with nearly 40 percent representing insider threat operations.

How the Scheme Works

Threat actors use generative artificial intelligence (genAI) to create LinkedIn profiles that attract the attention of job recruiters. The threat actors complete a virtual interview process, often using stolen identity documents to bolster their fake identity. They are then hired, typically for a remote IT position. Everything from the company's perspective seems to check out with this new recruit.

During onboarding, though, things typically take a turn. The new employee will likely have an emergency that requires

travel. He or she will request that their new work equipment—such as a laptop—be sent to a destination that doesn't match the address information they provided to HR during the hiring process.

This new location is usually a laptop farm where someone is paid to keep the

laptop on and connected to the Internet so the threat actor can access it remotely. Some of the individuals storing the laptops are doing so unwittingly, says FBI Special Agent Elizabeth Pelker, who is the Bureau's specialist on this activity and was also at RSAC.

Most of these individuals are recruited online to just host the laptops, thinking they are doing someone based in China a favor, Pelker adds. The Bureau will typically see one to two laptops at a location; on the extreme end, it has recovered up to 90 at one residence.

Microsoft, on the other hand, is tracking thousands of personas and identities used by North Korean IT workers, says Greg Schloemer, senior threat intelligence analyst at Microsoft, who was also at RSAC.

Once on the payroll, these threat actors might provide their contacts with access to the corporate network to install malware to mine for cryptocurrency, conduct credential theft, steal proprietary data, or conduct data extortion after being fired, Schloemer adds.

The FBI's Internet Crime Compliant Center (IC3) published an alert in January 2025, warning private companies of data extortion and sensitive data theft by North Korean IT workers. The advisory also cautioned about the threat of credential theft.

"North Korean IT workers could attempt to harvest sensitive company credentials and session cookies to initiate work sessions from non-company devices and for further compromise opportunities," the advisory said.

One concerning development of this threat, Schloemer says, is the potential for a relationship between the clusters of threat actors conducting this remote IT worker campaign and the possible theft of intellectual property and sensitive information related to defense, nuclear, and aerospace capabilities.

"We need robust detection and response recommendations so we don't end up in a future scenario where IT remote workers enable really critical national security theft," Schloemer adds.

Book Review

Teaching Cybersecurity

By Daniel Shoemaker, Ken Sigler, and Tamara Shoemaker. CRC Press. 228 pages; \$46.95.

In 2018, the Association for Computing Machinery (ACM) and the IEEE Computer Society (IEEE-CS) announced the publication of the *Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity (CSEC2017)*. The guidelines were developed under the leadership of the Joint Task Force on Cybersecurity Education and with the contributions of educators, industry professionals, and government representatives from around the globe.

CSEC2017 includes four components: an overview of the cybersecurity discipline to frame the curricular model, a presentation of the curricular framework and outline of the recommended curricular content, a highlight of industry perspectives on cybersecurity, and a discussion of issues related to the educational practice, suggestion for a process to develop roadmaps that link the curricular model to workforce frameworks, and references that highlight how global institutions could implement the curricular guidelines.

In *Teaching Cybersecurity: A Handbook for Teaching the Cybersecurity Body of Knowledge in a Conventional Classroom*, authors Daniel Shoemaker, Ken Sigler, and Tamara Shoemaker have written a book that is a tremendous resource for those tasked with implementing CSEC2017.

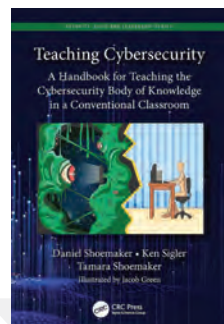
Many who are required to implement CSEC2017 are elementary school and high

school teachers who often don't have a background in information technology or cybersecurity, yet are tasked with incorporating it into their lesson plans. This book is meant for that population.

Written in a jargon-free and easy-to-read style, *Teaching Cybersecurity* gives the reader a good understanding of the eight domains of the common body of knowledge (CBK): data security, software security, component security, connection security, system security, human security, organizational security, and societal security.

Each chapter is a self-contained explanation of the CBK topic and can be used to teach the topic to elementary, middle, and high school students. The chapters also include exercises to facilitate meaningful discussions and insights about the topic.

Albert Einstein is quoted as saying, "If you can't explain it simply, you don't understand it well enough." While information security can be quite intimidating, *Teaching Cybersecurity* is a helpful guide to assist your understanding of the topic so that it can be taught well.



Reviewer: Ben Rothke, CISSP, CISM, CISA, is a New York City-based senior information security manager with Tapad who has more than 20 years of industry experience in information systems security and privacy. His areas of expertise are risk management and mitigation, security and privacy regulatory issues, design and implementation of systems security, encryption, cryptography, and security policy development. Rothke wrote Computer Security—20 Things Every Employee Should Know.

Flags to Look for

There are many benefits of having a remote workforce, but it also comes with some risks when you're only interacting with candidates online—especially ones trained to beat the system.

Schloemer says there are two facets to detecting these threat actors: technical indicators and behavioral indicators.

Technical indicators might include using a public VPN service, remote management tools, and other programs and tools

that are not typically allowed on corporate laptops. On the behavioral side, flags might include frequent excuses for not attending meetings, last-minute cancellations, and shifts in location.

“Some other behavioral indications that a remote employee may be a DPRK IT worker include noticeable variability in quality of work or knowledge,” Schloemer explains. “For example: high performance on interview, but low performance on the job. Or an individual writing quality code but then displaying an inability to explain how the code works—this might be an indication that multiple distinct operators are working the role behind the scenes.

“Additionally, look for different-looking individuals present on-camera in an interview process versus on the job,” Schloemer continues. “Organizations should also look for poor work quality—although, notably, some DPRK IT workers are quite skilled and may be very high performers.”

Organizations should also look for poor work quality—although, notably, some DPRK IT workers are quite skilled and may be very high performers.

Schloemer cautions that as the threat actors mature it is becoming more difficult to detect them. It’s critical to educate front-line managers about the tell-tale signs of this activity. These individuals should be most tuned into what their direct reports are doing, behavioral changes, and general work performance.

Monitoring an employee’s performance and engaging in tough conversations with that individual are the biggest mitigation challenges that CrowdStrike has identified

besides technical controls, Meyers says.

“A lot of managers don’t want to have those difficult conversations about performance,” Meyers explains, adding that a direct report might not be doing a great job but isn’t doing a terrible one either—they are skating by. “That’s something everyone should think about, and that’s a way to home in on these threats we’re seeing. We have to take that seriously as an industry and managers of people.”

Owning and Mitigating the Risk

There is the sense within the security community that the DPRK remote IT worker scheme risk is not its responsibility to own. James Robinson, CISO of Netskope, says that the consensus from many CISOs he’s spoken with is that this is a human resources problem that security needs to partner on.

The Society of Human Resource Management (SHRM) is a major professional association for HR leaders with 340,000 members



Rely on STI®



**Safety Technology
International**



...to help enhance
building security

Push Buttons with Optional Camera

The G3 and GF push buttons feature an optional IP camera. Upon activation, the dual-purpose button delivers critical alerts in emergency situations and provides real-time visual identification of individuals.

FEATURES

- Optional IP camera
- 6 color choices with optional protective covers
- Flexible mounting (flush or surface)
- G3 button reconfigures on site: Key-to-Reset, Momentary, and Turn-to-Reset

BENEFITS

- Captures video before and after button interaction
- 180° Field of View
- Visual identification of intruders, active shooters, and suspicious individuals
- Allows for immediate assessment of situations and surroundings

Learn more at sti-global.com
or call 248-673-9898

2025

See us at GSX booth 1419

in 180 countries. A spokesperson for the association declined to comment on the DPRK remote worker scheme and guidance it has provided members about the tactic.

Regardless of who ultimately owns the risk, there are steps that security teams can take to help protect their business and identify these threat actors.

When Robinson first learned of the technique a few months ago, he says he requested a briefing on it from his local FBI Field Office for himself, the head of HR, and his company's legal team. Netskope then began to put together an action plan to mitigate the risk of the threat. Robinson encourages other CISOs to take this same approach.

Other recommendations from the IC3 include conducting data monitoring, practicing the principle of least privilege on networks, and limiting privileges for installing remote desktop applications. It also suggests making changes to the remote-hiring process, including completing as much of the process and onboarding in person as possible.

Schloemer says that required in-person interaction can be an effective strategy against the threat actor that is looking for low-hanging fruit with few friction points.

"However, as we discussed during [RSAC], this is an especially agile and adaptable actor," Schloemer adds. "If an organization were to implement such an in-person requirement, the actor could certainly adapt its ecosystem of enablers so that someone could appear in person to collect a device or complete a stage of the background check."

There are more steps organizations can take to mitigate the risk of this tactic, including implementing identity-verification processes during interviews, onboarding, and throughout employment for remote workers, and cross-checking HR systems for other applicants with the same résumé or contact information.

"North Korean IT workers have been observed using artificial intelligence and face-swapping technology during video job interviews to obfuscate their true identities," the IC3 said in the January alert.

Additionally, organizations should consider reviewing applicants' communication accounts since North Korean IT workers have reused phone numbers and email addresses on applications that are supposed to be for different people.

During the interview process, interviewees should consider asking "soft" interview questions that lead to information about location and education background, since many North Korean IT workers have claimed to attend non-U.S. educational institutions.

The IC3 also suggested verifying third-party staffing firms your organization works with to ensure they are following these recommendations.

Third-party staffing firms are one of the largest vectors for these actors to gain access to your organization, Schloemer says.

"That hiring process is a black box. You don't have a lot of visibility into how that person was vetted," Schloemer explains. "It's worth having a conversation with them about this threat and do as much as you can to gain visibility into that process."

This could be especially important for companies looking to fill roles outside of the United States, where the threat actors might turn next, Pelker says.

"If you have a workforce not in the United States, make sure your partner teams are tracking this during recruiting, hiring, and as managers," Pelker adds. "And if you identify someone who checks those red flag boxes, reach out to us at [IC3.gov](https://www.ic3.gov). We also have teams of FBI agents across the world."

How each organization conducts these reviews of their workforces and handles this threat might look different because of their unique policies and regulations, but if they identify a DPRK remote IT worker in their workforce, the response should be the same, Schloemer says.

"Once an organization has reached a high degree of confidence that an individual among their workforce is linked to DPRK IT worker activity, the most important step is terminating the user's access to all systems and data as quickly as possible to prevent further compromise or disruptive and destructive action—like data theft or extortion," Schloemer explains. ■



PAR-KUT
INTERNATIONAL
WELDED STEEL PREFAB SECURITY BOOTHS
WWW.PARKUT.COM

See us at GSX booth 2314



Tell Me More



Connecting metrics with a human-centric narrative can make security's value proposition harder to refute.

By Sara Mosqueda

Sean Sportun was thinking about closing down one of the convenience stores he oversaw in Ontario, Canada.

Robbers had struck the Mac's Convenience Store in Thunder Bay eight times between January and March 2012. One of those instances involved three teenage robbers, who had a standoff with the police after trying to hold up the store at knifepoint. The store also abutted an alleyway where prostitutes and drug users often loitered, and its exterior walls were regularly graffitied.

A disciple of crime prevention through environmental design (CPTED), Sportun repeatedly ordered for any new graffiti to be removed or painted over within 24 hours of its appearance, authorized the installation of new cameras, and fenced off an area that provided bad actors an escape route.

But “no matter what we did to this store from a CPTED perspective of lighting, taking away exit points—you name it, we did it—it didn't work,” says Sportun, who at the time was the security and loss prevention manager for Mac's Convenience Stores. At this point, he considered shuttering the store altogether.

Instead, he decided to throw a party.

Calculating the Value of Community Outreach

In years prior, Sportun directed part of the loss prevention program to focus on community engagement efforts that also improved the company's relationships with the neighborhoods around its stores. He had seen success in a program where law enforcement provided coupons for free drinks to break the ice with local youths and reward them for positive behavior. Sportun had also heard of a crime prevention effort in Toronto where graffiti and murals were used to beautify neglected buildings.

So, Sportun decided to commission local graffiti artists to give the Thunder Bay site a facelift. With support from law enforcement, the store's landlord, the mayor, and other stakeholders, the artists completed the mural in May 2012. The design featured elements that the community said it wanted to see, such as sketches provided by local high school art students. To commemorate the mural's completion, the store hosted a party outside of the facility with music, performances, youth artists, food, and more.

“It worked,” Sportun says. The store no longer saw the robberies it had before, and Sportun decided to try the same

experiment at a different store. The second store had not been directly targeted, but it was near enough to areas where violent crimes had been committed that Sportun thought the project could result in a better relationship between the store and the community. And then he picked a third store for the mural project. After successes at all three stores, the project caught the attention of researchers at Harvard Business School (HBS), who helped provide funding for murals at additional stores, with 17 murals commissioned throughout the region by 2016.

The projects cost roughly \$2,400 CAD (\$1,850 USD) per site; however, researchers determined that stores with these murals saw an average sales increase of \$62,371 CAD (\$48,170 USD) per year. There were also reports of year-over-year decreases in the number of negative or violent incidents experienced at Mac's stores in central Canada. Incidents decreased from 139 in 2012 with \$54,243 CAD (\$54,275) in associated losses to 72 incidents in 2015 and \$9,914 CAD (\$7,770) in losses. There was a slight increase in 2016 with 87 incidents but a decrease to \$9,708 CAD (\$7,490) in associated losses.

The murals generated positive news around the Mac's brand, with the murals or the parties celebrating their completion often resulting in press coverage and essentially free advertising. Compare this to an average of \$1.2 million CAD (\$926,760) that Mac's spent on radio commercials that reached 60 percent of Ontario residents for 26 weeks, according to the HBS case study.

“There's a story to tell here because of the things that we've been doing, and the robberies have gone down drastically,” Sportun says.

He estimates that the art projects resulted in \$10.6 million CAD (\$8.2 million) in loss prevention savings. The decreased robberies also meant that employees were not injured on

If you're going to get 45 minutes a year with the CEO and his or her leadership team to tell your story, you better be able to tell it quickly and effectively.

the job and could safely work, avoiding productivity losses and impacts to the company's insurance premiums.

In their bare bones form, the numbers alone would not have told the full story. Sportun knew that for the project to continue its spread, he would have to present other landlords, his C-suite, and law enforcement with a compelling story. HBS researchers and Sportun created a document and a short film about the project, allowing Sportun to show others the impact of the project and how it could improve other sites.

Part of telling this story about crime prevention through community engagement was understanding how other Mac's departments and external stakeholders would find the numbers compelling.

Sportun notes that finding the right narrative and format helped convince others that the project could result in benefits to the company, landlords, law enforcement, and community leaders.

"Then, before we knew it, we had 25 of these things up. And it became a thing within the policing world where it was making it into their annual reports," Sportun says.

Police departments in other areas also reached out to him to ask if they could select a store in specific areas where another mural could be commissioned. "Not only did it start reducing incidents of criminality, but it started becoming a brand reputation thing," he adds, pointing to another benefit of the program.

Sportun is not alone in blending math and language to create a compelling story that can generate support and excitement for security. When applied by and to a security team, metrics can indicate how effective certain measures have been and whether they remain a worthwhile investment.

Targeting Useful Information

"Identifying the efficacy of a security program or solution is about measuring the quality of targeted results from the rich pool of information on our program performance," says George Campbell, an emeritus faculty member for the Secu-



Mac's Convenience Stores in Canada partnered with local police to support the StreetArt Mural initiative, using public art to build stronger community ties.

rity Executive Council, a research and advisory firm specializing in corporate security risk mitigation solutions.

At their core, metrics are data points that numerically or statistically reflect interactions and incidents.

"Metrics are the switches and dials for security program performance measurement," says Campbell, who was formerly CSO at Fidelity Investments. Metrics can be used to analyze, evaluate, and adjust the performance of a solution, team, department, or even an entire organization.

"Risk-related metrics not only direct security response planning and performance measurement but become the CSO's communication and influencing strategy," adds Campbell. "We need to leverage metrics to tell security's quality and value story."

When used effectively, the data can condense a story, giving security practitioners the ability to hit the highlights in minutes or even seconds—time that's valuable when you only meet with someone from the C-suite once a year.

The metrics should be able to tell the story quickly and with little to no need for an explanation. When done right, an executive viewing the data or graphics will be able to quickly comprehend the message they tell, understanding the performance and value of the product or system that the metrics represent, according to Dave Komendat, former vice president and CSO for Boeing, currently CSO and partner with Corporate Security Advisors.

“If you’re going to get 45 minutes a year with the CEO and his or her leadership team to tell your story, you better be able to tell it quickly and effectively,” Komendat says. “And the best way to do that is with value-added facts and data.”

These metrics need to show how an investment into security has resulted in a return on investment (ROI).

Campbell, who has been teaching CSOs—including Komendat—about metrics for decades, offers some tips on how to paint a picture with this data.

When you’re first looking for key metrics, Campbell recommends considering how well security vulnerabilities are being identified, along with analyzing if actionable metrics are helping achieve an adequate resolution.

“If we can’t deliver solid information here, we are failing in our basic responsibility to communicate and engage management,” Campbell says. “This is our value story and what management must hear.”

Security leaders should also focus on identifying key risks and pinpointing what key performance indicators (KPIs) are tied to those risks. These KPIs should have currency and staying power, so they can be adapted to evolving

risks. For example, some KPIs today would likely be indicative of cyber threats, regulatory risks, climate change impacts, and business resilience.

Lastly, Campbell recommends engaging with key stakeholders and inserting yourself into the conversation on business risk strategy and management. Understanding other departments’ and key players’ motivations and goals will help you craft a message or story from the data that resonates beyond security.

“Understand the part or parts we can play in enabling the board’s strategic and enterprise risk management objectives,” Campbell says. “Focus key program delivery with metrics that clearly demonstrate how our programs are contributing to the success and the health of the enterprise.”

The Power of a Human Angle

Before retiring from Boeing, Komendat says that one of his goals was ensuring the C-suite and the company at large

ACCESS & POWER INTEGRATION...



RACK MOUNT

HARDENED OUTDOOR ENCLOSURE

See us at GSX booth 2155

viewed the security department as a business enabler instead of a cost center.

“I wanted leadership in the Boeing company to know that I and my team understood and supported the strategy of the company,” he says.

To achieve this, Komendat focused on metrics that demonstrated value instead of ones focused on activity. Activity metrics indicate a count, such as the number of calls answered by a company’s global security operations center (GSOC). However, the number of phone calls or alerts placed to a GSOC is unlikely to adequately demonstrate the value presented by the GSOC. Komendat would instead highlight the responses to these calls. How many of these calls were related to an issue with production, a medical emergency, or a critical incident? These metrics would showcase how the GSOC provides support for business continuity and employee safety—supporting the larger mission of the organization.

Getting these numbers and stories to leadership can help a team secure new resources when necessary and even retain them when the larger organization is struggling. Komendat recalls using metrics to show executives why the company

If we can’t deliver solid information here, we are failing in our basic responsibility to communicate and engage management.

maintained an on-site fire department. The fire department, which also provided emergency medical services, would get called upon more than once a year to respond to a medical emergency on the production floor, he says.

“If you were having a cardiac event and I am putting an EMT next to you with an AED within three minutes, you have a 70 percent chance of surviving that event,” he says.

But without the internal EMTs, who are familiar with the physical layout of the facilities, the employee would not get medical care as quickly.

“On their best day, it’s going to take them 6 to 9 minutes to get into the facility. They’re going to have to find the per-

...ENDLESS POSSIBILITIES

Altronix®



WALL MOUNT

TROVE™ lets you design and deploy your preferred brand of access control with Altronix power solutions in virtually any environment.

- Simplifies board layout & wire management
- Reduces installation and labor cost
- Scalable for any size system
- Available as pre-configured and pre-wired kits

Streamline your access control deployments with TROVE™. Only from Altronix.

Run With It™

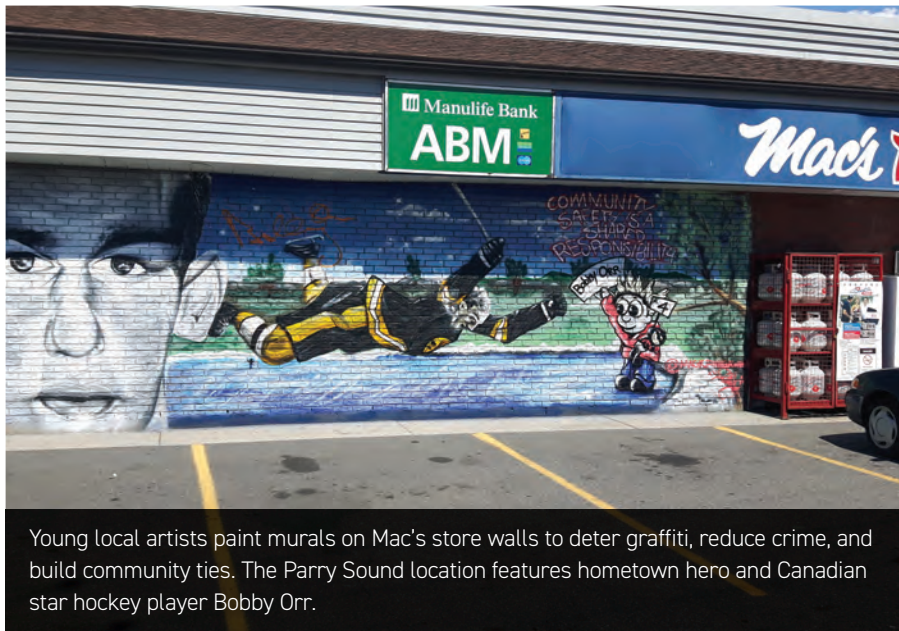
son. We have huge, complex facilities,” Komendat says.

And if it takes 6 to 9 minutes for help to arrive and treat someone experiencing a cardiac event, the chance of survival decreases significantly.

The impacts extend beyond the possibility of one death. There are also going to be side effects on other employees—co-workers and friends of the colleague who just died will likely experience some trauma. But by maintaining the internal fire department, those same employees are likely to see company emergency responders saving a life and administering care.

“That is a powerful, impactful scene. And it’s a powerful, impactful metric when you start to get pressure,” Komendat says.

While contractual obligations provide another strong reason to keep an internal team in the face of budget cuts, it doesn’t resonate as strongly as the employee retention and employee goodwill borne from a real-life medical drama. This is on top of the other work performed by this internal team, such as cleaning up hazardous materials.



Young local artists paint murals on Mac’s store walls to deter graffiti, reduce crime, and build community ties. The Parry Sound location features hometown hero and Canadian star hockey player Bobby Orr.

“That’s a positive brand—that’s ‘the company cares about me’ type of response. So, being able to articulate and tell stories like that are important,” Komendat says.

Because when you can talk about how the surviving employee came back to work days or weeks later, how their teammates didn’t need to use PTO or bereavement leave to deal with the trauma, and how the surviving employee and their family visited the EMTs to thank them for saving his or her life, it strikes an emotional chord with leadership.

“It sounds corny, but it wins,” Komendat says. “And who’s going to sit there after hearing a story like that and go, ‘Hey, you’ve got to take \$10 million out of your fire budget?’ Nobody does that.”

This approach is reflective of a larger scale need—that security metrics must become more proactive rather than reactive, according to Campbell.

“The threat landscape, regulatory compliance, and the demands of more risk-aware and engaged boards of directors have driven this evolution,” he says. ■

Sara Mosqueda is associate editor for *Security Management*. Connect with her on LinkedIn or send her an email at sara.mosqueda@asisonline.org.



Visit Splan at GSX Booth #736

Enterprise Visitor Management & Next Gen. PIAM

AI-Powered Security & Access Solutions

Our Enterprise Visitor Management and Unified Identity and Access Management (PIAM) solutions leverage AI-driven insights to streamline security and simplify access.

- ✓ Contact us for more information - info@splan.com
- ✓ For Support Queries - support@splan.com

+1510-320-3305

www.splan.com



See us at GSX booth 736

WHEN FACED WITH A POTENTIAL THREAT, DO YOU WANT
YOUR ONLY ASSESSMENT CAPABILITY TO BE AN HOUR AWAY?



THE vonLOEWENFELDT GROUP WILL HELP YOU STAND UP YOUR OWN TEAM TO
RESPOND TO, ASSESS, AND MITIGATE THE THREAT,
OR PROVIDE EXPERT BOMB TECHNICIANS WITH EXTENSIVE OPERATIONAL EXPERIENCE.



Frameworks of Support

Armed security officers are trained to respond to threats in seconds, but are they prepared to handle the weight of that responsibility?

By Megan Gates



Taking
today's
keys into
tomorrow



The original developer
and world leader of
electronic key control



**MORSE
WATCHMANS**



GSX Booth # 2301
Global Security Exchange
Sept. 29th - Oct. 1st, 2025
Ernest Morial Convention Center
New Orleans, LA



Armed security officers train to respond to a threat in seconds, sometimes making life-altering decisions in the blink of an eye to draw their service weapon to protect themselves and other people in their care.

Many of these officers will go their entire career and never use their firearm while on duty. But some do have to take that action. One such case occurred this past year at a poultry processing facility in the United States.

An employee at the facility had been let go. As he exited the plant, however, he stopped at his vehicle, retrieved a rifle, and opened fire in the parking lot. He then walked toward the facility's perimeter gate and guardhouse, continuing to fire his weapon.

The security officers on duty heard the rounds and immediately reacted. A supervisor provided cover for a newly trained officer on her first day at the site, helping her shelter on the floor behind a concrete wall. The supervisor then took cover behind a guardhouse, stepped out, saw the gunman pointing the rifle at him, and neutralized the threat with his service weapon before anyone else could be harmed.

"Our officer neutralized the threat immediately, then had the forethought to recognize he needed to survey the scene, make sure there's no other threats, and secure the scene until law enforcement got there. That same officer started directing per-

sonnel, getting them out of the way, getting them away from the scene itself," says Edward E. "Gene" Sanders, COO of DSI Security Services. "That officer exhibited all the training that he had had—not only being able to neutralize the threat with what he learned on the firing range but to also control a very chaotic situation with what he learned in incident control."

The officer's actions likely saved many lives—including his own—at the facility, which employed several hundred people. The incident demonstrates the seriousness that must be taken when training security personnel to carry and use firearms on the job.

Sanders is extremely familiar with this training process. His career began in law enforcement, and then he transitioned to working with DSI in 1991. About 15 years ago, he obtained and continues to maintain the rigorous National Rifle Association (NRA) Law Enforcement Firearms Instructor certification. Sanders also obtained credentials that allow him to instruct security and law enforcement officers on firearms use.

The incident at the poultry plant "makes you realize that on any given day, we have 5,500-plus security officers out there on post, and the vulnerabilities that are out there, the risks that are out there and that are present," Sanders says. "It confirms just how important and how serious training should be taken and should be administered."

Your future is in security.

You're stepping into an exciting new chapter—and ASIS is here to support your transition from the public sector into a rewarding role that leverages your unique skills and experience.

Tap into your potential with our free, personalized tools that help chart your career path and turn your military or law enforcement background into security success.

Start your journey today.



Client Education

When arming a security officer, it's important to keep in mind the purpose for doing so: armed security is often seen as a deterrent. Thieves or other malicious actors might see an armed security officer at a store, for instance, and decide they should target another location that doesn't have a guard standing by to potentially intercept them.

"It's really more about that officer presence and being a deterrent to somebody breaking the law, stealing that piece of property, or assaulting that individual," Sanders says.

Several factors go into deciding whether armed security is needed at a site. These include the location of the site, the crime in the area, the risk analysis, and the product or people you're seeking to protect.

"Generally, in the banking industry, you'll see [armed security] quite often," Sanders says. "In the retail industry, you'll see it frequently. Then in areas that are known to be high-crime areas or known to be very vulnerable, then you'll incorporate an armed security officer as that deterrent."

It's critical to educate the client, however, to make sure he or she understands the differences between law enforcement and armed security personnel.

"They may think that an armed security person can carry out the exact same duties and exact same responsibilities with the level of force that a police officer or law enforcement officer can, and unfortunately that's not completely accurate," he says.

Law enforcement, for instance, is trained to enforce the law and has a much broader authority to use deadly force when necessary to do so. Certified peace officers—private security officers who have been commissioned by a government entity but are employed by a private company—may have more latitude to use deadly force because they are also enforcing the law in their posts. But generally, contract security officers have the same right to use deadly force as regular civilians do, Sanders explains.

I think the number one thing for me is safety because you're responsible for every person around you.

"In the security arena, the ability to use deadly force is directly associated with the presence of imminent bodily harm or damage, or death, to yourself or to someone else," he adds. "That's the difference between the two. Law enforcement still has that requirement, but beyond that they can use weapons to enforce the law—certain levels of the law. Then you have to go back to the force continuum, which dictates how an officer—whether it's contract security or whether it's law enforcement—what level of force they can use."

Private security officers also have an assignment, often a post location, to protect a customer and that customer's property. This differs greatly from law enforcement, which can move more

The 5 Steps in a Use-of-Force Continuum

Like law enforcement agencies, private security organizations typically have policies that outline how officers can use force while on the job.

These policies are sometimes referred to as the use-of-force continuum. They include the levels of force appropriate for a situation and how a security officer might move from one level to another to respond in the moment. These policies help ensure that officers are responding to threats in a lawful and proportional manner.

Here are what the five levels of a typical use-of-force continuum look like in theory, based on examples from the National Institute of Justice.

- 1. Officer presence.** Security officers are present at a physical location to act as a deterrent. Officers are encouraged to have professional and nonthreatening attitudes.
- 2. Verbalization.** Officers issue calm, nonthreatening commands to another person—like asking to see the person's ID badge or ticket to enter a restricted space. If the person does not comply with the request, an officer might raise his or her voice and issue shorter requests—like "stop" or "don't move."
- 3. Empty-hand control.** If someone does not respond to a security officer's verbal requests or if there's a need for a physical intervention, security officers could use empty-hand control techniques. These include restraint holds or physically escorting an individual away from the area.
- 4. Nonlethal force.** If empty-hand techniques are not effective or appropriate for the situation, security officers may use nonlethal force to subdue or control an individual without causing permanent injury. This could include using a TASER, a baton, or pepper spray.
- 5. Lethal force.** As a last resort, security officers can use lethal force—such as a firearm—when they face an imminent threat of death or serious bodily harm to themselves or others. This use of lethal force is very highly regulated and demands a significant escalation in the threat level, such as an active shooter situation.

It is critically important to clearly communicate and train security officers on the continuum and appropriate use of force, so they respond to threats in a lawful and appropriate manner.



STRONGPOLES
SECURITY MOUNTING SOLUTIONS

MADE IN USA

Don't Settle for a Repurposed Light Pole. Choose the BEST.

- Security Camera Poles
- Building Mounts
- Indoor Mounts
- Keypad Pedestals

Designed to withstand 195 MPH winds! STEADYMAX

ENDLESS COMBINATIONS

NEWEST PRODUCTS

HD PARAPET MOUNT WITH JUNCTION BOX

FLAT ROOF PARAPET ADAPTER

KEYPAD PEDESTAL W/ OVER WATCH CAMERA

Aluminum Equipment Cabinets

SCAN ME

Call Today 844-669-3537

StrongPoles.com

Home of the SteadyMax - The Most Rigid Pole in the World

freely within its jurisdiction to pursue threats or use force.

Additionally, when incidents occur police officers or sheriff's deputies can call their colleagues for backup. Security officers, however, rely on law enforcement to be their backup.

"To be effective with both armed security and law enforcement, you have to bridge the gap in that relationship because both of us are partners, both of us have common goals, and both of us have responsibilities and can assist each other," Sanders says.

Training and Firearms

In most cases, armed security officers are issued handguns—typically a semi-automatic 9mm or .40 caliber. Security officers who transport high-value assets, such as jewelry or cash in an armored vehicle, might be issued shotguns. Sanders adds that private security officers who work in corrections facilities or transport inmates might also be issued shotguns.

"A lot of times in those environments, you would see the need for a shotgun because it is a weapon of choice when you're in close proximity to the potential threat or you have concerns with the impact to your surroundings," Sanders says. "If you're in an area where there's a number of personnel, you would seek something like a shotgun versus a handgun simply because it's more of a short-range type of weapon."

These are powerful and lethal tools that security practitioners may use in the course of their work. For Sanders, the most important thing is understanding the weapon that you're using and your responsibility for it.

"You have to recognize the risk and the responsibility of [carrying a firearm]," he adds. "I think the first order of business in any weapons training is getting familiar with the weapon—the nomenclature of that weapon, understanding its components, how it works, and understanding the safety piece of it."

The safety aspect is paramount. Not every firearm operates in the same way. Safety mechanisms are likely to be different, along with loading and discharging.

"If you have a revolver, it's completely different than when you have a semi-auto," Sanders says. "I think the number one thing for me is safety because you're responsible for every person around you."

Additionally, security officers should be familiar with how to break down their service weapon and clean it safely.



“All guns are different. Some guns are cleaned differently than others. Some require less oil for lubrication. Some require more,” Sanders says. “At all times, when you’re cleaning a weapon, there are never rounds in the area where you’re cleaning the weapon. The weapon is separated. It’s clearly broken down.”

After security officers are familiarized with how the firearm works and its safety mechanisms, next up is becoming proficient with handling and firing it. This includes the basics of sight alignment, trigger squeeze, and all the components that go into using the weapon accurately, Sanders adds.

This should be followed by education on the use-of-force continuum and understanding how security officers can use force both legally and ethically, along with the ramifications of using that force. The use-of-force continuum, for instance, begins with the mere presence of the officer, escalating to less-than-lethal tactics, and then lethal tactics in certain situations. Officers should be educated on this continuum and then undergo scenario training so that when they are out on the job and a situation arises, they are prepared to properly handle that incident with the appropriate use of force.

Law enforcement and armed security personnel are asked to make split-second decisions that are life-altering, so Sanders says it is imperative to understand the use-of-force continuum and be trained, repeatedly, so they make good decisions.

“You’re trained in that situation. You know that situation, so you know how to respond,” he adds.

One technology that is assisting with this curriculum is simulation training. Many law enforcement agencies already use simulators to train officers, and Sanders says that DSI has used them at a local training center for law enforcement.

“In a simulation, your targets are different. They change. Then you have to quickly discern if that target is a threat or not a threat,” Sanders explains. “If the target is a threat, is it presenting a lethal threat—deadly force to you? Then, how do you properly respond to it?”

Sanders adds that it is essential to assess the mental health and psychological condition of the officer who is carrying a weapon.

“A lot of states right now—especially where we operate in armed security—have requirements that before the state will issue that armed security officer a license to carry a weapon, they have gone through that mental health evaluation and been approved and fit for duty,” Sanders says. “That’s typically how we are able to vet our potential candidates for armed services.”

Total training requirements for armed security officers will vary by jurisdiction. Most U.S. states require personnel to complete initial training, then go through refresher training—sometimes called requalification—within 12 months of being certified and every 12 months after that with the firearm that they are issued.

Twenty-eight U.S. states and the District of Columbia have specific training requirements for armed security officers, compared to 23 and the District of Columbia for unarmed security officers,

according to a 2021 white paper from the National Association of Security Companies (NASCO).

On average, the initial training requirement for armed security officers is about 40 hours. Twenty-three states also require continuing education and range qualifications each year for officers to maintain their license.

At DSI, for instance, the company has both on-staff and contracted instructors that work to train personnel, typically every six months and no less than every 12 months, Sanders adds.

“And not just on the caliber weapon that they’re carrying, not just the brand—whether it be Glock, Beretta, or Smith & Wesson—but they are actually training and certifying with the weapon that they are going to be carrying in their holster,” he says.

One state that maintains a high level of training requirements for armed security officers is Florida. It has an online platform that provides guidance on certifications and their validity and indicates whether administrative actions are being taken against a certification holder.

“They have what Florida calls D license for unarmed personnel and G license for armed personnel,” Sanders says. “They communicate with us frequently on any administrative action that might take place. Then, when renewals are coming up, they clearly articulate the training that needs to be done—the range and scores that have to be met.”

Off-Duty Storage

Armed security personnel should carry their assigned weapons only when they’re on duty and assigned to their post. Sanders says DSI requires its officers to use a Level 2 and above holster for their service firearms. This means that there is a level of retention to the holster that requires two means to get access to the weapon.

“They have to be able to press a button that releases the weapon and then pull that weapon out,” Sanders explains. “Some Level 3s have a finger release—a thumb release—and then you have to pull the weapon out.”

When preparing to come on duty, officers are responsible for making sure their weapon is ready for duty. This could include charging the weapon, checking for rounds, and loading it.

Once their shift is over, Sanders says officers are instructed to store their firearm in the trunk of their vehicle, where it cannot be accessed by the driver until he or she returns home. He recommends using a vehicle gun safe or gun box to store the firearm. Once home, that weapon is required to be stored in a

safe—preferably a biometric safe—and, when possible, where the rounds are securely separated from the weapon itself.

“Our primary concern is if an officer, for some reason, needs to store the weapon that they have the means by which to unload that weapon properly,” he adds. “In places that we have armed services—at a site—and the weapons are retained at the site, the weapons do not go home.”

In these situations, there needs to be proper weapons storage that includes a safe and clearing barrels where weapons can be cleared securely, Sanders says.

“One of the best ways to control or to safely manage a weapon is to always control that weapon,” explains Sanders. He has heard stories of officers in the industry taking off their duty belt with their firearm attached when using the restroom and then forgetting to pick it back up again.

“It’s happened both in the law enforcement arena and security arena,” he says. “It’s really about making sure they understand just the severity and the responsibility they have in control of that weapon, and always attending to that weapon at all times.”

Providing Support

Carrying a firearm as a security officer is a significant responsibility. If an officer needs to use that firearm in the course of their work, Sanders adds that it is imperative there is a process in place to debrief that officer and then provide him or her with support.

At DSI, for instance, the protocol for post-incident response involves gathering as much information as possible about what happened and ensuring that there is an independent investigation into the incident. This is sometimes handled by law enforcement or a state official. At the same time, the officer involved should be isolated to make sure he or she is physically okay and can provide a statement. DSI will then work with law enforcement to ensure the officer is supported while the investigation continues into what occurred.

“Once law enforcement has cleared it, we will typically put our officer on leave with pay to make sure that it was a justified situation,” Sanders says.

After that justification threshold is met, DSI also ensures the officer is made aware of employee assistance program benefits so he or she can get any necessary therapy support. Sanders says it’s important to encourage the officer to talk about the situation as best he or she can and to support the individual.

“If it’s an event that was justified and their actions save lives, everybody’s going to be thanking them, recognizing them for what they did, but at some point, that starts to dwindle,” Sanders explains. “Then you have the employee left with the event that just took place and whatever action they had to take.”

In the aftermath, Sanders adds that it’s important in this moment to use your HR resources to provide support to the officer.

At DSI, “HR takes the lead on that and through our different means of employee assistance, we get them the help they may need to be able to process what happened,” Sanders says. ■

Megan Gates is editor-in-chief of Security Technology. Connect with her at megan.gates@asisonline.org or on LinkedIn.



SECURITY TECHNOLOGY

More About Security Weapon Selection

Want more information and content about selecting the right weapons and equipment for security teams? Check out the full series online using this QR code.

PILOTED REMOTELY

MONITORING EVERYWHERE

Turn-Key Remote Piloted Drone Solutions

Experience comprehensive aerial monitoring and security, FAA-licensed remote pilots, autonomous patrols, and 24/7 monitoring—all included in one monthly fee.



DRONE SOLUTIONS - MONITOR MORE, MANAGE LESS

[TPCSECURITY.COM/DRONES](https://tpcsecurity.com/drones) | 913.441.0911



New Extremes

In some roles, working in high temperatures can be inevitable. But changing temperature ranges can make jobs increasingly dangerous without appropriate mitigation strategies.

By Sara Mosqueda

We usually think that extreme weather and temperatures are limited to rare areas or instances—the Gobi Desert, the North Pole, Tornado Alley, or an errant blizzard or heatwave.

But when it comes to how weather can harm humans, it doesn't take too much to qualify as extreme, especially when it comes to heat. Granted, what may feel hot to residents in Scotland might be considered downright balmy to those living in the southwestern United States. However, if someone isn't accustomed to actively working in what feels like hotter weather, prolonged exposure can result in a case of heat illness.

Heat illness is more than just sweating a little more and feeling uncomfortable in the heat. Most of the time, the human body subconsciously takes actions to remain in homeostasis—keeping everything inside stable and on an even keel regardless of the external environment. For example, if our blood sugar is too low, we get hungry and perhaps crave something sweet. Keeping our body temperature within a certain range is a big part of homeostasis, with bodies essentially operating as living thermostats. If things get too cold, we shiver in order to generate some level of heat through movement and muscle activity. If things get too hot, we produce sweat because as it evaporates, the departing moisture cools the surface of our skin.

But if someone is working in construction, patrolling outdoors for hours on end, or working in a factory with little to no air conditioning, there's only so much the body can do.

Mercury Rising

Although heatwaves are one of the most dangerous natural hazards, the death and destruction they cause are not always immediately noticed. As a result, the impacts may receive less attention than the instant swath of destruction cut by a tornado or tsunami.

According to a 2021 study, *Global, regional, and national burden of mortality associated with non-optimal ambient temperatures from 2000-2019: a three-stage modelling study*, more than 489,000 heat-related deaths happened every year. Of all heat-related deaths, 45.81 percent happened in Asia, 36.54 percent in Europe, 11.61 percent in the Americas, 5.22 in Africa, and 0.82 percent in Oceania. Heatwaves in particular cause spikes in deaths, evidenced by the more than 70,000 people who died during a 2003 heatwave in Europe.

Heatwaves have also been increasing in frequency and intensity in recent decades. “Between 2000 and 2016, the number of people exposed to heatwaves increased by around 125 million,” according to the World Health Organization (WHO). U.S.-based research also confirmed this increase, noting that among major cities the average in the 1960s was two heatwaves per year, but the number has grown to more than six per year during the 2020s. “The average heatwave season across 50 major cities is 46 days longer than it was in the 1960s,” the U.S. Global Change Research Program reported.

The bottom line: Hotter days are here to stay. So, people who work in the heat will need additional protections.

Anyone working outdoors or in indoor spaces that lack sufficient cooling and ventilation can be at risk for a heat-related illness. And it's not just heat that contributes—high humidity, which prevents sweat from evaporating, and high nighttime temperatures can exacerbate the conditions for heat-related illnesses. The constructed environment also factors in. Heat is absorbed by buildings, roads, and other infrastructure, meaning that temperatures can be 1 to 7 degrees Fahrenheit warmer in urban areas compared to the areas surrounding a city, according to the Center for Climate and Energy Solutions (C2ES).

Even short periods in high-heat conditions can affect judgment and physical performance—crucial traits in the security industry.

Heat-related illnesses are caused by exposure to extreme heat and are basically the result of the body's inability to sufficiently cool itself off, impacting the cardiovascular and respiratory systems, as well as kidney functions. This category of illnesses includes heat rash, heat cramps, heat syncope, rhabdomyolysis, heat exhaustion, and heat stroke. The most serious of these is heat stroke, which happens when the body can no longer control its own temperature.

“The body's temperature rises rapidly, the sweating mechanism fails, and the body is unable to cool down,” according to the U.S. Centers for Disease Control and Prevention (CDC). “When heat stroke occurs, the body temperature can rise to 106 degrees Fahrenheit or higher within 10 to 15 minutes.” If someone suffering from heat stroke doesn't receive emergency treatment, it can result in a permanent disability or death.

While solutions to preventing heat-related illnesses may seem obvious—stay inside, stay hydrated, stay cool—they are not always available or apparent.

For security officers who actively patrol large outdoor areas, such as campuses or parking lots, excessive heat can mean dehydration, fatigue, and heat-related illnesses. These effects “can seriously impair a security officer's ability to remain alert, respond quickly, and make sound decisions,” says Eddie Sorrells, CPP, PCI, PSP, the CEO of DSI Security Services. “Even short periods in high-heat conditions can affect judgment and physical performance—crucial traits in the security industry.”

Security officers stationed outside in the heat for prolonged periods are most at risk, particularly if they are exposed to direct sunlight or high humidity. The increased time and exposure to heat while unable to effectively cool off increases the risk of developing a heat-related illness.

“I think anybody that's ever been exposed to a level of exertion in extreme heat knows the physical and mental impact

that it took upon you or can take upon anyone,” says David LaRose, CPP, CPHA (Certified Healthcare Protection Administrator), national director of healthcare security for Garda World. “...If you’re not aware of your environment and the impact it can have on the officer physically and mentally, then we’re setting ourselves up for failure.”

Beyond duty of care, individual performance, or government regulations, employers might also be interested in recognizing, preventing, and treating these impacts because of a larger bearing on an organization. Staff turnover increases when an organization or industry doesn’t take care of its employees, including when it comes to hazards like extreme heat, according to Brent O’Bryan, senior vice president of global training and talent development for Allied Universal.

“It needs to be about the employees first. And we know that if it’s not, we’re going to lose people. So, we’ve got to make sure up front we’re doing the right thing—and that starts with recognizing some of the issues that weren’t recognized in the past,” O’Bryan says.

Mitigation and Response

Because extreme heat can significantly impact the efficacy and health of security patrols, especially those who work outside for significant stretches of time, proper management and training of those officers can make a substantial difference in an officer’s performance, health, and influence beyond their company and the client he or she serves.

Whichever policies and training security officers’ employers use to help promote safety and awareness during hot days, employers need to communicate and coordinate these needs and protocols with the clients the officers will be supporting.

Along with providing site-specific safety briefings for the officers to address any unique elements in the environment they will be working in, Sorrells notes that DSI also requests or negotiates with clients for officers to have access to air-conditioned spaces or water stations, as well as establishes the expectations for breaks, adjustments to uniforms when necessary, and limits on shifts to prevent excessive exposure. These kinds of discussions can help clarify clients’ needs and expectations of officers’ responsibilities while placing limits where needed.

While these steps may sound onerous, it can help to remember and remind clients that the additional measures can assist in decreasing turnover and increase retention, O’Bryan says.

“Our clients want to see the same faces. We want to have the same individuals out there who know what to do day in and day out,” he explains.

These discussions do not only occur during a contract negotiation; instead, regular meetings with clients allow the organization to review recent events. “Incidents could include how many heat-related issues have happened at this facility or location, and then we can adjust and work with



Types of Heat-Related Illnesses

Heat cramps

This is the mildest type, consisting of painful muscle cramps and spasms that occur during or after intense exercise and sweating in high heat.

Symptoms include painful muscle cramps, especially in the legs, and flushed, moist skin.

Heat exhaustion

This is more severe, resulting from the body’s loss of water and salt. It occurs when the body cannot cool itself properly. If left untreated, it can turn into heat stroke.

Symptoms include muscle cramps; pale, moist skin; a fever greater than 100.4 degrees Fahrenheit or 38 Celsius; nausea; vomiting; diarrhea; headache; anxiety; or feeling faint.

Heat stroke

The most severe form of heat illness, heat stroke is a life-threatening emergency that requires immediate medical attention.

Symptoms include warm, dry skin; high fever, usually greater than 104 degrees Fahrenheit or 40 Celsius; rapid heart rate; loss of appetite; nausea; vomiting; headache; fatigue; confusion; agitation; lethargy; or stupor. In severe cases, seizures, coma, and death are possible.

that client on what changes we need to make going forward,” O’Bryan says.

To support keeping security officers safe even while having to work in the heat, it can help to conduct training that emphasizes how to recognize and respond to heat stress and to enact policies that include regular cooling and hydration breaks. Another way to improve resistance to excessive heat is by modifying uniforms and equipment to compensate for the increased temperature.

Policies and Training

Implementing and leveraging a heat illness awareness and prevention plan can be a valuable investment.

“To ensure officers remain safe while still meeting the needs of our clients, training protocols must be adjusted during hot weather months,” LaRose says. Training ahead of those warmer days should include recognizing the early signs of heat stress, such as dizziness, nausea, excessive sweating, and confusion.

Training should also include how to handle instances of heat stress or heat-related illnesses once they are identified. If an officer is suffering from heat exhaustion or sees someone else exhibiting signs of a heat-related illness, training should address how and where he or she can be moved to, as well as providing an environment where the person can fully recover and rehydrate. Training at Allied Universal notes that thirst is an early indicator that someone is headed toward dehydration.

“That’s back to that prevention and early warning signs—that’s part of the training. It’s how to take care of yourself,” O’Bryan says.

Proper training can prevent a situation from happening or at least keep a situation from worsening. “You have to respond really quickly because things can—no pun intended here—heat up quickly in those dangerous situations,” O’Bryan adds.

When a serious heat incident happens, it can significantly affect organizations’ reputation, workers’ morale, and liability risks. U.S. employers are required to report any fatalities due to a heat-related illness to the U.S. Occupational Safety and Health Administration (OSHA) within eight hours, and inpatient hospitalizations must be reported within 24 hours. This means that instances of heat stroke, rhabdomyolysis (muscle injury and breakdown), and any kidney damage because of severe heat or dehydration would be reported. A report could trigger an investigation into the causes of the heat-related illness and depending on the circumstances and outcome, OSHA might send an investigator to assess the workplace and identify hazards.

To counter some of the impacts from excessive heat, DSI has implemented certain safety protocols that are built into broader officer training and daily operations, according to

Sorrells. These include hydration practices, with officers trained to hydrate before, during, and after a shift, as well as the employer providing access to water or beverages with electrolytes in locations where the heat is a factor.

Remote monitoring with GPS and wellness checks are also used for outdoor or remote posts so officers can report heat-related issues as they happen. The system allows supervisors to monitor officers’ patrol routes and issues alerts if there is a defined period of inactivity. Sorrells adds that he expects shifting climate patterns will increase the need for and use of drones and remote surveillance measures to help reduce human exposure to extreme heat.

Training in anticipation of extreme heat can be multifaceted, relying on various formats to support real learning so the information is both accessible and memorable.

“It could be a document that they can read and refer back to,” LaRose says. “It could be a briefing before staff is deployed. ...It could be a formal part of the training.” LaRose also issues special bulletins related to seasonal issues or risks, and he advises pairing them with refresher sessions during regular briefings.

It needs to be about the employees first. And we know that if it’s not, we’re going to lose people.

If an event involving extreme heat or a heat-related illness occurs, the debriefing of the incident can also contribute to training. Beyond understanding the incident and collecting the facts regarding it, officers can benefit from leaders recognizing when proper performance came into play and how things can be improved. “Maybe it’s because of the training something was observed, it was immediately handled, and the outcome was positive. And it reflects back to the training of the officer,” LaRose says.

At Allied, officers and supervisors also use an internal learning management system for training, with monthly safety topics incorporated into regular learning sessions. The topic for May 2025 was heat illness prevention, providing all employees with a refresher session of a more in-depth course that all employees must complete during their first 21 days at the company. Similar to Garda World, the company also provides other learning methods, such as a short video—the idea being that multiple educational avenues can help in communicating with and educating employees, according to O’Bryan.

Everyone that *Security Management* spoke with said that their training and policies regarding extreme heat were created to at least meet or exceed regulations set by OSHA and other regulatory agencies. This means that every site is required to have a heat illness and prevention plan, and every

employee's onboarding training includes a section on heat illness and prevention. But they also pulled lessons from other industries and from internal data regarding previous incidents. Sorrells adds that for DSI, their programs are created in partnership with several voices outside of traditional security—legal counsel, operational leaders, and risk management experts. “This cross-functional approach ensures that our protocols are both effective and legally sound,” he says.

LaRose, O'Bryan, and Sorrells all said that their organizations provide their officers with first aid training in response to heat stress and related illnesses. This allows them to not only identify and treat any stress among security officers, but also provide assistance to anyone on the properties they help secure.

Clothing and PPE

“There are other things that I think sometimes are overlooked that really give a value add. That's whether the uniforms are correct for the climate,” LaRose adds.

Once the temperatures start to rise, it's time to at least consider switching up the work wardrobe for outdoor workers. For warmer days, choose a uniform consisting of lighter, breathable materials instead of the suit and tie that would be standard on cooler days or in a setting with air conditioning. Some clothing and hats also offer protection from harmful UV rays, further protecting officers in the long run. Depending on the setting, it may be worthwhile to see if additional equipment can help keep officers cool while on the job.

Both the material and the color of clothing can help mitigate against warmer weather. For example, wearing white in the summer to protect against heat is common. However some studies show that, counterintuitively, wearing black in some conditions—particularly if the clothing is loose-fitting and there is at least a mild breeze—can have a cooling effect. As for materials, in general you should select lightweight woven fabrics. Different materials have different moisture absorption proper-

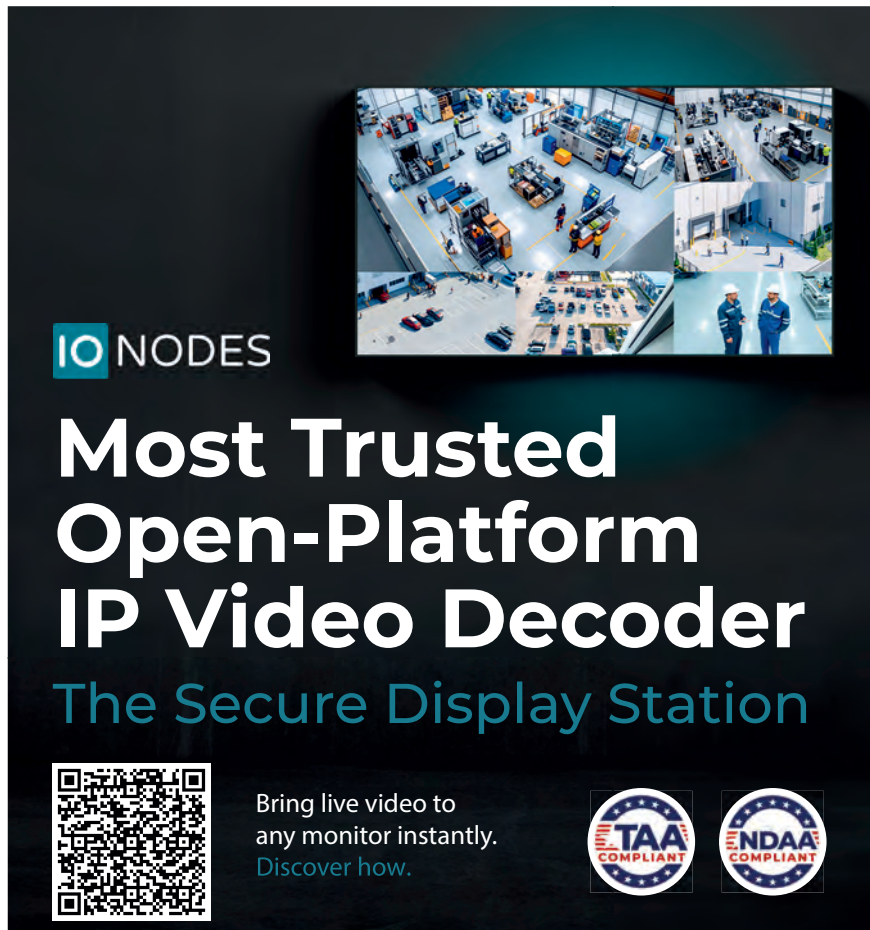
ties that can help determine that material is better in different environments. For example, in dry environments, high-absorption cotton may keep security officers cooler than other fabrics, while in humid environments, moisture-wicking synthetics will be the cooler option.

Consideration of materials should also extend to any accessories, such as utility belts or vests. Vests are often necessary gear to protect the wearer from weapons, but on hot days the material that covers the plates should also be breathable instead of one that retains heat, LaRose advises.

Along with breathable or ventilated clothing, Sorrells also recommends providing cooling towels and portable fans when and where it is appropriate.

Other personal protection for security patrols can include a neck gaiter, sunglasses, sunscreen, and accessories that can offer protection from the heat, sun, glare, and UV rays, O'Bryan adds. ■

Sara Mosqueda is associate editor for *Security Management*. Connect with her on LinkedIn or send her an email at sara.mosqueda@asisonline.org.



IO NODES

Most Trusted Open-Platform IP Video Decoder

The Secure Display Station

Bring live video to any monitor instantly. Discover how.

TAA COMPLIANT NDAA COMPLIANT

The October 2023 Hamas attack in Israel and its aftermath sparked a new era of campus free expression and protest. Many institutions, including Saint Louis University, had to grapple with how to respond.

By Melinda Heikkinen

Meeting Peace *with* Peace





Saint Louis University campus

There is a long-standing history of student activists demanding social change through protest on college campuses.

From the student-driven removal of Harvard College's president in 1639, through the civil rights and anti-war demonstrations of the 1960s and '70s, to the anti-apartheid demonstrations in the '80s, college and university students have always been a force for change.

Most institutions of higher learning have well-developed policies and processes when it comes to allowing free expression. But the events of 7 October 2023 sparked a new era of free speech that set many schools on their heels—forcing not only a deep assessment of what free expression was, but a reckoning with how to respond to it both within the values of the institution and the expectations of the law.

On that day in October, Hamas and its supporters launched an attack on Israel from Gaza, killing 1,200 Israelis and taking 240 hostages. The inevitable Israeli Defense Forces counterattack into Gaza has killed tens of thousands of Gazans and stirred up outrage across many American communities.

Finding themselves at the epicenter of much of the protest activity, colleges and universities have had to make hard decisions on how to respond. While each institution was presented with unique circumstances and made their decisions based on those circumstances, the results were of varying success.

In July 2024, *The New York Times* reported that more than 3,100 people were arrested in relation to protests at college campuses across the United States. Many of the charges associated with these arrests were dropped, but university administrators remained on edge. In addition to the fallout generated by arresting activists, many campuses experienced weekslong encampments and extensive property damage. But other universities and colleges also experienced protests, demonstrations, and free expression events that—while they undoubtedly caused disturbances—did not result in arrests.

Some of their success in these situations was because they had the experi-

ences of other universities to reflect on. Much like the golfer who is second to putt, these administrators got to see the effectiveness or ineffectiveness of the line chosen by the previous institution's administrators. But some of these institutions' officials simply choose a different path, which could be instructive to other administrators as they work to ensure the security of their communities.

One such organization is Saint Louis University (SLU) in St. Louis, Missouri. This story of SLU's journey through the spring semester of the 2023–2024 academic year provides an example of how collaboration and partnership can effectively limit long lasting effects of protests gone wrong.

The Clock Tower Accords

SLU has a history of unique responses to community free expression. Established in 1818, the Jesuit, Midwestern university touts that the concept of social justice is at the very core of its values. It encourages its students to stand up for those in need while respecting the ideas of others.

The challenges of this stance came to light in October 2014 after a police officer killed Black teenager Michael Brown in nearby Ferguson, Missouri. Tensions were further exacerbated by the shooting of Vonderrit Myers, Jr., the son of a SLU employee, by a police officer working as private security shortly after. More than 1,500 people, including students, faculty, and staff, participated in a protest march that ended at SLU's clock tower, a focal point on the campus.

While most of those involved participated in a general protest activity, some began to set up an encampment, which the university's administration allowed to stay. As expected, there was tremendous pressure to physically remove the individuals involved. Safety, security, and hygiene concerns were all expressed, but the people participating in the encampment were peaceful. Instead of having them physically removed, the administration actively engaged in daily conversations to gain a better understanding of what the protestors wanted. The result was what has become known as the Clock Tower Accords, a signed commitment by

the university to inclusion and social justice. The 13-point accords concluded six days of peaceful occupation at the campus clock tower. This course of action also set the tone for future protests.

Fast-forwarding 10 years to the pro-Gaza/Palestinian protests of 2023–2024, SLU was no different than other institutions in that it had to maneuver through accusations of anti-Semitism and Islamophobia, pressure from the community to stop all protests, and a push to allow unlimited free expression. Social and political challenges existed as well; students, faculty, staff, and alumni tended to strongly support one side or the other in the conflict, causing significant stress on attempts to come together to discuss issues.

It was not lost on the university community that safety and security had to be a primary focus as they maneuvered through these

Demonstrators listen to speakers during a rally on the campus of Saint Louis University on 13 October 2014 in St. Louis, Missouri.



challenges. SLU administrators reached back to the responses to the clock tower encampment and rapidly engaged in collaborative efforts—not to stop the protests but to enable free expression while ensuring the operations of the university were hindered as little as possible.

A Proactive Protest Plan

Upon receiving word of an initial protest early in November 2023, SLU administrators mobilized a small team of professionals to respond. The team, composed mostly of public safety staff supplemented by student affairs, marketing, and communications personnel, provided guidance to the participants and monitored the protest. It was apparent early on that this

would be a recurring event in the coming months, signaling the need for a more robust and formal response team.

A larger group of staff and faculty members was immediately brought together. The mission of this group—which included public safety leadership alongside participants from emergency preparedness, campus operations, university counsel, marketing and communications, and student affairs staff—was to identify, plan for, and implement pre-intervention, event response, and post-intervention processes. From a security standpoint, the intent was to expand beyond a traditional stance of response-only and engage with known participants to proactively diminish the impact on campus operations.

Observers attending the first protest were able to identify participating students and community leaders. This gave

Collaboration and partnership can effectively limit long-lasting effects of protests gone wrong.

the pre-event intervention team the ability to initiate conversations that clarified university processes and expectations, assessed the cohesiveness of the protestors, and—possibly most importantly—built trust by actively listening to what the protestors wanted. This was the first and most significant success in SLU's semester-long journey. These students became willing to give university officials notification of upcoming protest events, making it possible to take necessary steps to protect campus operations.

Post-event teams mirrored pre-intervention activities by actively engaging with protest participants, talking through incidents and challenges that may have occurred during the event, explaining why certain actions were taken, and offering additional support. This was especially effective because it signaled to protestors that although efforts were made to curtail their impact on campus operations, the university was willing to listen and, where possible, take action centered on the activists' goals.

SLU's public safety department functioned as the response team, staffing the events with senior leadership, up to 20 field officers, and an emergency preparedness team working out of an emergency operations center (EOC). Student affairs and communication staff supplemented the officers assigned to work the protest, but public safety leadership took the lead. Though SLU's public safety department is armed, it is not a sworn police department, which somewhat limits actions it can take.

For example, department officers could take someone into custody but could not



The team could not ignore the fact that there could be attempts to set up an encampment or take over a building.

directly cite the individual for any municipal code violations. Due to successful pre- and post-event collaboration, law enforcement presence was not requested for most of the protests on SLU's campus.

Public safety personnel accompanied by student engagement personnel met with the protest leaders at every protest, advising them that violence, calls for violence (including property damage), and threats of any kind would not be tolerated. Protesters were also advised that if they needed assistance, such as first aid or breaking up fights, it would be given.

Behind the scenes, several buildings were locked, and public safety personnel were posted there to assist those who genuinely needed access. The buildings locked were selected due to potentially high impact to campus academic operations and to protect university VIPs.

Many protestors were very angry that they had been denied access to those spaces. They felt that—as paying students—they should have the right to access any building they wanted, anytime they wanted, for any activity they chose. On this point university officials stood their ground, clarifying that while they were committed to free expression, they would also take steps to limit the overall impact on campus operations and the activities of those not participating in the protest. The practice was repeated in subsequent events, and protestors significantly limited their attempts to occupy space inside buildings.

Changing Tactics for Escalating Tensions

SLU's approach to free speech and protest events proved to be very successful throughout the semester. However, St. Louis area protestors shifted their college campus approach on 27 April 2024 significantly, raising the angst of university leadership once again. On that day, protestors made several attempts to set up an encampment at the nearby Washington University, resulting in more than 80 arrests.

Protest organizations began to call for similar actions on SLU's campus, and eventually a protest was planned for 1 May 2024. What complicated the matter further was the active participation of local government officials in the protests. These officials were associated with SLU in one way or another, intensifying the pressure on planning teams by adding political pressures. This was to be a true test of what many considered SLU's unconventional approach to these types of events.

SLU's protest team had a short period to plan for this event and relied on its previous successes as the anchor for the university's response strategy. The team could not ignore the fact that there could be attempts to set up an encampment or take over a building. Being less than three weeks from commencement when the campus would be visited by thousands of family members and friends, the pressure on university leadership was immense, but the university stood by its commitment to collaboration.

University leadership met with government officials who would be participating and discussed potential actions. Public safety staff engaged with local and federal law enforcement to obtain as much intelligence as possible and to coordinate response. Pre-event intervention teams reached out to their contacts to gather information and offer alternatives to protesting students. All information was shared internally and resulted in the university staying the course with its approach to protests—with one distinct difference.

Unlike other protests on SLU's campus where SLU students took the lead, there was the potential that this one would be led by non-students. All coordination was being made with student groups, but there was a question as to whether they could retain control of the event. SLU officials were confident that student activists' leadership limited the potential for significant property damage, attempts to occupy buildings, or create encampments. If an external group took control, there was great concern about property damage and an attempt to set up an encampment—as had been the case at Washington University a few days earlier.

A second factor that SLU's protest team took advantage of was the fact that students were genuinely concerned about being arrested. To address both these factors, the team coordinated far more extensively than usual with the St. Louis Metropolitan Police Department (SLMPD).

Overall, SLU stuck to its tradition of allowing and supporting free expression. Many faculty and staff marched to show support for their students and back them up if others attempted to take over the protest. Public safety officers conducted themselves in the same manner protestors had become used to.

Unlike in previous protests, though, university leadership maintained a presence in the EOC to be able to make decisions and give direction quickly. SLMPD leadership posted with SLU's public safety leadership, and traffic control units from the police department quietly positioned themselves at strategic locations in case protestors attempted to block the main city street running through campus. A contingent of city police officers was placed on standby to respond only if needed. Police personnel were not visible to any of the protestors. The intent of their presence was not to intimidate but to be strategically positioned to respond quickly if SLU officials requested it.

The second change was the distribution of public statements from SLU and St. Louis city leaders about the planned protest.

SLU President Fred Pestello, PhD, sent a letter to the SLU community committing to allowing a peaceful protest on campus. In this letter, he explained:

"I write today to share—and emphasize the need for—a sense of calm and a commitment to our Jesuit mission and values. As we did in October 2014, we intend to meet peace with peace, permitting our students to engage in advocacy while ensuring that the work of the institution continues."

Pestello continued by reinforcing the expectation of conduct of those participating in the protest.

St. Louis Mayor Tishaura Jones also issued a statement addressing the planned protest and defining SLMPD's role in any response. She reinforced that the SLMPD would only be used if university officials requested the department, and she committed to the community that force would not be used on non-violent protestors.

Put to the Test

On 1 May 2024, just before 6:00 p.m., hundreds of protestors began to gather at

the clock tower. The protest that ensued lasted several hours. Protestors marched around campus. They then moved to Grand Avenue—a main city thoroughfare that runs through SLU's campus—and blocked it. Because of all the pre-coordination, SLMPD traffic enforcement was able to quickly divert traffic around the group, resulting in little inconvenience to commuters.

For approximately an hour, the protestors chanted, shared stories, and called for action. A small group of counter-protesters stood nearby silently, holding Israeli flags. SLU's public safety department monitored all activity, ready to intervene if necessary. After the last speaker, a hush came over the crowd, and many of the protestors lined up to pray. After prayers, the protestors stood, gathered their things, and marched back to the clock tower where they peacefully dispersed.

Saint Louis University's consistent approach to protests and free expression

demonstrations proved to be effective for multiple events that occurred over a seven-month period. While this is not the only approach organizational leadership can take when addressing protests and demonstrations on or near their facilities, SLU has a long history of community engagement and the resources to implement it. Individual organizations faced with this type of activity must take action that is appropriate for their specific circumstances. But SLU's approach shows that, when possible, collaboration with both internal and external parties can have a positive effect on the ultimate outcome of these types of events. ■

Melinda Heikkinen is the associate vice president/chief for public safety and parking and cards services at Saint Louis University. She served as the senior public safety official leading protest response on the university's campus during the 2023–2024 academic year.



IONODES CitySafe

CREATE SAFER AND STRONGER COMMUNITIES

IONODES CitySafe is a Community Safety Video Sharing Platform to securely share live and recorded video from local partners with law enforcement Real-Time Crime Centers (RTCCs).

PERCEPT Gateway

Secure Cloud Platform
*No Storage

Genetec RTCC

Get in touch to learn more.



The Changing Landscape of the Physical Security Industry

By Boudewijn Pesch, Vice President of Japan and Asia-Pacific Channel Sales at Verkada

For decades, physical security for businesses was largely defined by hardware – analog cameras, Digital Video Recorders (DVRs), and incremental improvements in resolution, compression, and low-light performance. Innovation moved gradually and was siloed across distinct sub-systems such as video surveillance, access control, communications, and intrusion detection. But the industry is now in the midst of a far more profound transformation.

Over the past five years, several concurrent technological shifts have fundamentally changed how security solutions are deployed and used within the modern enterprise. The transition from analog to Internet Protocol (IP) video may have marked the beginning, but the next wave – driven by cloud,

artificial intelligence (AI), and data convergence – is reshaping the industry's foundation.

Shift #1: From On-Premises to Cloud-Native

The first and most visible transformation is the widespread adoption of the cloud. Just as enterprises have moved their core applications – customer relationship management (CRM) tools, enterprise resource planning (ERP) software, communications, and analytics – to cloud platforms, they are now demanding the same from their physical security systems. The exponential growth of data centers globally stands as a testament to this shift. Cloud architecture delivers more than scalability and uptime – it provides centralized management, easier updates, remote accessibility, and significantly enhanced resilience. Security is no longer tied to a physical server room; it lives in

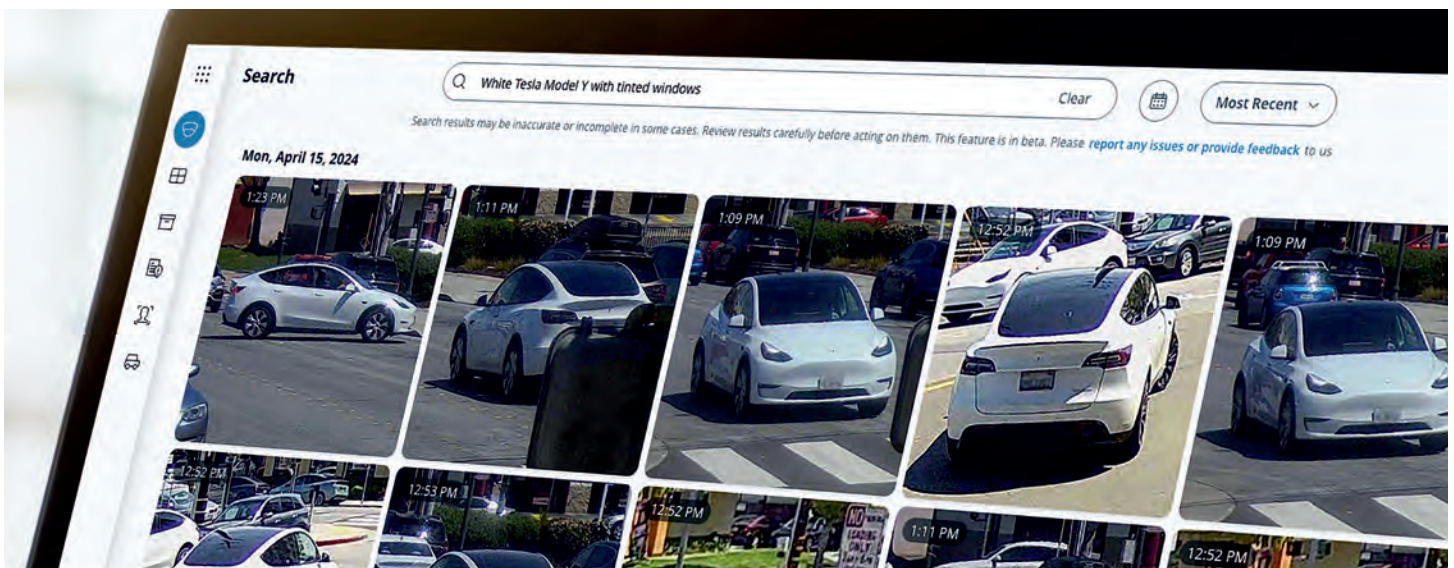


Boudewijn Pesch, Vice President, Japan and Asia-Pacific Channel Sales at Verkada.

the same digital fabric as the rest of the enterprise.

Shift #2: From Intelligent Automation to Artificial Intelligence

The industry has long used basic forms of intelligent automation – motion detection, line crossing, or object classification. But today, AI is redefining the very outcome of what security systems can deliver. At the heart of this transformation are Vision Language Models (VLMs) – advanced AI systems that can interpret video footage through natural language. Deployed across hybrid cloud architectures, VLMs empower users to run forensic and real-time investigations using freeform queries like “person in a red jacket near



With Verkada AI-Powered Search, users can search for specific footage with natural language like “White Tesla Model Y with tinted windows,” to quickly find relevant clips in minutes.

Advertisement

the loading dock yesterday.” These models scan millions of video frames to identify visual matches and deliver actionable insights in seconds.

When integrated with access control logs, building telemetry, and other systems, VLMs enable a unified situational awareness layer – transforming security from a reactive measure into a proactive source of business intelligence.

Shift #3: The Democratization of Security

The sheer number and variety of devices – cameras, sensors, alarms, and readers – have made traditional system management costly and complex. Modern enterprises no longer tolerate siloed, high-maintenance infrastructure. They demand simplicity, scalability, and insights at the edge. This demand is driving what I call the “democratization of security,” making intelligent, enterprise-grade security accessible and manageable across departments and geographies. It’s not just about better tools – it’s about empowering every stakeholder, from security operators to IT administrators, and employees, with real-time visibility and control.

Shift #4: From Cost Center to Value Creator

With this democratization comes an inflection point: the integration of physical security with broader enterprise IT systems. When security data feeds into operational dashboards, HR systems, point of sales platforms or workplace analytics, it becomes a business asset – not just a safeguard. As a result, security transitions from a pure cost center to a strategic function that can reduce costs, optimize workflows, and in some cases, even drive new revenue streams. Think of examples like integrating with POS platforms to detect fraud, using occupancy trends

to optimize building management systems, or combining video data with CRM logs to analyze visitor engagement and space utilization.

A Call for Responsible Innovation

Of course, with great capability comes great responsibility. The ability to analyze and match individuals or vehicles with high accuracy using AI raises critical issues of privacy and ethical governance. To safeguard trust, the industry must

By aligning with vendors who prioritize long-term customer success and reward loyalty, integrators can scale their impact – delivering not just systems, but business outcomes, and being recognized for the trust and value they bring to every engagement.

The winners in this next chapter of physical security will be those who embrace the transformations in the industry including cloud-native and AI-powered solutions. And those

“The future of security is not only about who builds the best camera – it’s about who turns complexity into clarity, and risk into insight.”

establish structured controls – access management, audit trails, query moderation, and transparent data policies. Responsible use is not optional – it is foundational.

What This Means for Partners

For integrators, this transformation presents a powerful opportunity. As security shifts from standalone systems to intelligent, cloud-connected platforms, those who evolve from installers to trusted advisors will unlock long-term value. The winners will be those who build deep customer relationships, deliver integrated outcomes, and guide clients through digital transformation.

Manufacturers with a strong focus on enablement, education, and scalable platforms are empowering partners to succeed in this new era. Through advanced training, certifications, and support for advanced services, the right partners can grow beyond the traditional project model and tap into recurring revenue streams.

who champion ethical innovation and simplicity.

Because the future of security is not only about who builds the best camera – it’s about who turns complexity into clarity, and risk into insight.

See How Verkada is Shaping the Future of Physical Security

Visit Booth #3113 at GSX for a live look at our newest AI-powered innovations that make it easier to keep people and places safe.



Designed with simplicity in mind, Verkada offers six product lines: video security cameras, access control, environmental sensors, alarms, workplace, and intercoms.

Three New ASIS Standards in 2025



The year 2025 has been an exceptional one for ASIS International standards, with the association releasing three new standards: *Investigations*, *School Security*, and *Executive Protection*.

Each ASIS standard is designed to provide detailed guidance for security practitioners across the industry on how to conduct aspects of security programs in accordance with industry best practices.

The revised *Investigations Standard* provides a framework for the investigations process, from establishing a program to conducting individual investigations. It outlines the necessary principles, processes, and best practices to ensure that investigations are conducted impartially, objectively, and in compliance with applicable legal and ethical guidelines.

The new *School Security Standard* provides a comprehensive framework for a school security program that includes physical security, behavioral threat assessment and management, and emergency operations planning. It addresses assessing risk and developing protective

strategies for applying security measures necessary to support and promote safe K-12 educational environments.

The new *Executive Protection Standard* provides a framework for determining the need for an executive protection (EP) program, as well as how to develop, implement, operate, and maintain an effective EP program. It provides guidance for the assessment of threats, vulnerabilities, and risks to the protectee; the identification and justification of protective services; and delivery of support based on industry accepted risk management principles.

Learn more about these and the many other high-quality standards and guidelines ASIS has developed at asisonline.org/standards-guidelines/.

ASIS standards and guidelines are available to members as free eBooks and at a 50 percent discount for soft-cover editions.

The ASIS Awards of Excellence

ASIS International is committed to honoring outstanding achievements and nurturing the next generation of leaders through the ASIS International Awards of Excellence. Congratulations to all our 2025 winners!

President's Award of Merit

- Jeffrey A. Slotnick, CPP, PSP
- Ralph "RC" Miles, CPP
- Timothy M. McCreight, CPP

Don Walker Memorial CSO Center Security Executive Award

Allen J. Innis, CPP

E.J. Criscuoli, Jr., CPP, Memorial Volunteer Leadership Award

John Richards, CPP, PCI, PSP

NextGen of the Year Award

Jonathan Perillo, CPP, PCI, PSP, CISSP

PCB Outstanding Achievement Award

Meshal Ayed Aljohani, CPP, PCI, PSP

Ralph Day Memorial Security Officer Heroism Award

Jonathan C. Langley

Roy N. Bordes, CPP, Memorial Community Leadership Award

Coleman L. Wolf, CPP, CISSP

Women in Security Global Community Karen Marquez Honors

Elizabeth Moslander, CPP, CBCP

Distinguished Service Award

- Meshal Ayed Aljohani, CPP, PCI, PSP
- Per Lundkvist, CPP, PCI, PSP

I.B. Hale Chapter of the Year Award

- Doha, Qatar
- Jamaica
- Kuala Lumpur, Malaysia
- Mexico City
- San Francisco Bay Area
- Venezuela

Outstanding New/Revitalized Chapter Award

Spain

YOUR WEAKEST POINTS CAN BE YOUR **STRONGEST DEFENSE**

Fortify glass doors and windows with retrofit security glazing that resists forced entry without replacing existing systems.

IMPACT  **SECURITY**
A LIMITED LIABILITY COMPANY

DEFENSELITE[®]
BULLET  **SHIELD**[™]

VISIT US AT BOOTH 2508

EXHIBITOR

GSX
GLOBAL SECURITY EXCHANGE
29 SEPTEMBER - 1 OCTOBER, 2025
NEW ORLEANS, LOUISIANA, USA

Contact us for a threat level assessment: 888-689-5502 • defenseelite.com • info@defenseelite.com

ASIS Global Board OF DIRECTORS

PRESIDENT

Joe M. Olivarez, Jr., MBA
Jacobs
League City, TX, USA

PRESIDENT-ELECT

Eddie B. Sorrells, CPP, PCI, PSP
DSI Security Services
Dothan, AL, USA

SECRETARY/TREASURER

Pablo Colombres, CPP
GIF International
Sao Paulo, Brazil

CHIEF EXECUTIVE OFFICER

William W. Tenney
ASIS International
Alexandria, VA, USA

AT LARGE DIRECTORS

Axel Petri, CPP
Deutsche Telekom AG
Bonn, Germany

Lisa Oliveri, CPP, PCI
Washington, DC, USA

Karen Frank, CPP
KPMG
Raleigh, NC, USA

Rick Kelly, CPP
Chubb
Mechanicsburg, PA, USA

C. Joshua Villines, CPP, PCI, PSP
Human Intelligence Group
Atlanta, GA, USA

Wilson Esangbedo, CPP
Nigerian Institute for Industrial Security
Lagos, Nigeria

EUROPEAN REGIONAL BOARD

Andy Williams, CPP
Crilly Consulting, Ltd.
London, United Kingdom

NORTH AMERICAN REGIONAL BOARD

Mark Folmer, CPP, PSP
Robotic Assistance Devices
Montreal, QC, Canada

LATIN AMERICA CARIBBEAN REGIONAL BOARD

Marco A. Vega, CPP
COTECPRO
San Jose, Costa Rica

ASIA PACIFIC REGIONAL BOARD

Danny Chan
Mastercard International, Inc.
Singapore

Community of the Year Award

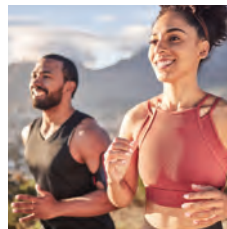
Enterprise Security Risk Management
(ESRM) Community

ASIS Foundation Virtual Fitness Challenge Success

The ASIS Foundation 2025 Fitness Challenge recently concluded after an excellent run, bike, and swim. The campaign raised more than 150 percent of the donation goal thanks to the generosity of ASIS members and security industry supporters from around the world.

With these charitable contributions, the ASIS Foundation will be able to continue its mission to serve the security industry through scholarships and research. The foundation gives out more than 100 grants and scholarships each year to support continuing growth and education for security industry across the globe. It also supports industry research on contemporary threats, best practices, and regulations.

Thank you to our Fitness Challenge sponsors: Arslan SRS, Black Mountain Solutions, Lady Askari, Lares Risk Management, Ledlow Security Group, SAGE Integration, SGT-Risk Management, stappone, and Thermal Radar.



Introducing: Operation Career Change

ASIS has worked with veterans and retired law enforcement from seven nations to develop to develop free resources that can transition a career of service into private security career success. Operation Career Change includes career maps for specific military and law enforcement positions and ranks to show how skills learned during service align with civilian security roles.

Guidance is currently available for U.S. Army, Air Force, and Navy veterans, as well as U.S. federal law enforcement and

U.S. metropolitan law enforcement. Guidance is coming soon for U.S. Coast Guard and Marine Corps veterans.

This framework serves as a foundational template that can be adapted and implemented worldwide, enabling global expansion of veteran and law enforcement career support programs.

Learn more at asisonline.org/professional-development/operation-career-change.

Get Involved with Your Community

The ASIS annual Call for Volunteers is open now through 15 October.

Volunteering with ASIS is a great way to grow your professional network, develop leadership skills, and contribute meaningfully to the profession. If you are passionate about what you do, we invite you to help ignite that passion in others.

Whether you are new to the industry or have been a security management professional for decades, we have opportunities for you to give back and make a difference.

Learn how you can get involved with ASIS at asisonline.org/volunteer.

70 Years in Security

ASIS International is excited to celebrate 70 years as an association. In February 1955 the very first ASIS Board took office, and since then the organization has grown to more than 34,000 members across more than 150 countries. Through the diligent work of our members and volunteers, ASIS has been able to produce industry-leading standards, create four certification programs for professionals at every career stage, and constantly generate educational content like webinars and certificate courses.

In that very first year, ASIS also hosted its first Annual Seminar, later renamed Global Security Exchange (GSX). That makes 2025 the 70th anniversary of GSX, too! Every attendee, speaker, and exhibitor from the past seven decades has contributed to the great event that GSX is today.

Thank you to all the security practitioners who have made the last 70 years possible—we could not have done it without you! Here is to the next 70 years of excellence. ■

Body-Worn Camera Solution with Milestone XProtect®

Live Video Streaming and Evidence Management

- Open-Platform, ONVIF
- High-Quality Wide-Angle Video
- 4G LTE / Wi-Fi Connectivity
- Live Video Streaming
- Bi-Directional Audio
- Geolocation on Live Map
- Ruggedized Design
- 12h+ Work Shift Battery
- Secure Evidence Management



Get the live
demo experience.

GSX
Visit Booth #719



XProtect
Evidence
Manager



Judicial Decisions

Cybersecurity. The U.S. Securities and Exchange Commission (SEC) reached a settlement agreement in principle with SolarWinds Corp and its chief information security officer (CISO), which would end litigation concerning a massive cyberattack.

The SEC sued SolarWinds in October 2023, claiming it misled investors about the risks in its systems that left it vulnerable to cyberattacks—including the 2020 SUNBURST breach. In that incident, Russia-linked hackers infiltrated SolarWinds's systems to ultimately penetrate clients' networks.

In July 2024, a U.S. federal judge dismissed most of the SEC lawsuit against SolarWinds. Nearly a year later, the SEC, SolarWinds, and its CISO—Timothy Brown—asked a U.S. federal judge to stay further court proceedings while the parties finalize and approve a settlement.

The parties will file settlement paperwork or provide a status update by 12 September, according to a letter sent to Judge Paul Engelmayer, who is overseeing the case. (*SEC v. SolarWinds Corp., et al.*, U.S. District Court for the Southern District of New York, No. 23-cv-09518-PAE, 2025)

United States

Discrimination. To settle a lawsuit filed by Students Against Antisemitism, Harvard University agreed to adopt a broader

definition of anti-Semitism when dealing with discipline cases and its nondiscrimination policies. The amended definition now aligns with that of the International Holocaust Remembrance Alliance.

The school also agreed to hire an administrator to advise on all complaints pertaining to anti-Semitism, prepare a public annual report that details Harvard's response to discrimination or harassment, host an annual symposium focused on anti-Semitism at American universities, and provide training to students and staff on recognizing and combatting anti-Semitism. (*Alexander Kestenbaum and Students Against Antisemitism, Inc., v. President and Fellows of Harvard College*, U.S. District Court for the District of Massachusetts, No. 24-cv-10092-RGS, 2025)

Harvard entered into a separate confidential settlement agreement with the Louis D. Brandeis Center for Human Rights Law and the center's Jewish Americans for Fairness in Education. The settlement was similar to the one with Students Against Antisemitism in that the universi-

ty agreed to use the broader definition of anti-Semitism in the school's nondiscrimination policies and will hire a consultant to assist with anti-Semitism complaints.

These settlements are separate from the ongoing legal battle that Harvard is engaged in with the Trump administration over alleged civil rights violations.

Targeted violence. A New York jury found a New Jersey man guilty of attempted murder in the stabbing of noted author Salman Rushdie in 2022.

On 12 August 2022, Hadi Matar attacked Rushdie while he was speaking at an event in Chautauqua, New York. Matar stabbed Rushdie several times across his body, including in one of his eyes. Grievously wounded, Rushdie was hospitalized and ultimately lost the use of one of his hands due to severed nerves, as well as losing sight in his right eye.

The jury also found Matar guilty of assaulting Henry Reese, who had been moderating the discussion with Rushdie at the Chautauqua Institution event and tried to stop the attack. Earlier in the court proceedings, Matar, who was arrested by law enforcement present at the August event, pled not guilty to the charges.

In May 2025, a judge for Chautauqua County sentenced Matar to the maximum prison sentence for a second-degree attempted murder charge—25 years. The judge also sentenced Matar to a concurrent seven years in prison for injuring Reese. (*People of New York v. Hadi Matar*, Chautauqua County Court, 2025)

Matar is also facing federal charges of terrorism because of the attack.

Legislation

Australia

Weapons. A temporary ban was placed in Victoria prohibiting the sale of machetes throughout the state ahead of its planned changes to the Control of Weapons Act.

The ban became effective in late May after a fight at a shopping center broke out between two rival gangs that involved machetes. The ban defines machetes broadly as large-bladed cutting knives, although kitchen knives are exempt from the ban.

The ban is expected to be lifted with the enactment of the amended Control of Weapons Act in September 2025, at which



29 SEPTEMBER – 1 OCTOBER, 2025
NEW ORLEANS, LOUISIANA, USA

THANK YOU FOR BEING PART OF GSX 2025.

We look forward to seeing you in
Atlanta, 14–16 September 2026.



point the ban will be replaced with the new law that will altogether outlaw the sale or possession of machetes.

Through an amnesty program, anyone in possession of a machete has three months from the law's enactment to surrender the weapon in designated boxes at police stations.

Hungary

Mass gatherings. The Hungarian government can now ban public events hosted by LGBTQ+ communities, such as Pride parades.

Lawmakers claim that the law, which was approved by the Hungarian Parliament along party lines (140 for, 21 against), is helping protect children's rights to moral, physical, and spiritual development. In recent years, the current government campaigned against LGBTQ+ communities, claiming that its policies concerning the protection of minors are necessary to guard against what it calls woke ideology.

Critics of the law see it as not only a way to curb the rights of those within the LGBTQ+ community, but also as another move that brings the government closer to authoritarianism. The law also empowers authorities to use facial recognition tools to identify anyone that attends banned events.

A separate aspect of the amended law is the government's ability to temporarily suspend citizenship of any Hungarian dual national if authorities determine the individual is a threat to the public or national security. The suspension could last for up to 10 years if the person is determined to present such a threat.

Prime Minister Viktor Orbán's government has previously taken steps to guard itself from alleged foreign entities that present a threat. Orbán has continued to target his critics, including media outlets, civil rights activists, and anti-corruption groups, which the prime minister claims have received financial support from international donors.

U.S. States

Gun violence. Illinois will now require the removal of firearms from people accused of committing domestic violence if the victim is granted an order of protection against his or her abuser.

Under Karina's Law (HB 4144), law enforcement must promptly remove guns,



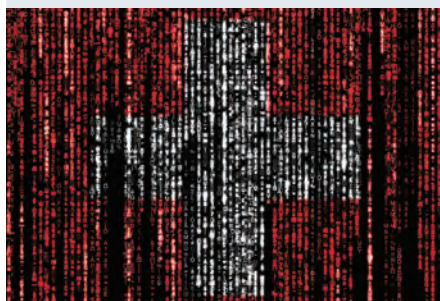
International Regulations

Switzerland

Critical infrastructure. The Swiss National Cyber Security Centre (NCSC) enacted a new regulation ordering critical infrastructure operators to report cyberattacks within 24 hours of discovery.

As of 1 April 2025, owners and operators must report any cyberattacks that "endanger the functionality of the affected critical infrastructure, has led to manipulation or leakage of information, or is associated with blackmail, threats, or coercion," according to the NCSC.

The new mandate, which amended the nation's Information Security Act, affects owners and operators in sectors like drinking-water suppliers, energy, finance, healthcare, telecommunications, and transportation. If an entity discovers a cyberattack, it can file a report on the NCSC's Cyber Security Hub or via email using a form on the NCSC website.



If owners or operators can only provide incomplete information about the attack in the initial report submitted, they have 14 days to complete the report.

Those who fail to report a cyberattack can be fined. The Federal Council will implement legislation regarding the fines on 1 October, giving organizations six months to prepare and familiarize themselves with the reporting obligations before fines can be levied.

firearm parts, and firearm identification and licenses from someone who has a restraining order against him or her, because that person's Firearm Owner's Identification card would be revoked by the order. Once a judge has issued a search warrant for the person's home, law enforcement must search for and remove these items within 96 hours.

Prior to the law, there was a loophole in confiscating firearms from an alleged abuser because it was unclear who was responsible for the removal of the weapons and their accessories.

Illinois Governor JB Pritzker enacted the law on 10 February. It was named for Karina Gonzalez, who was given an order of protection against her husband weeks before he shot her, their daughter, and their son. Only the son survived and has since lobbied for the passage of the law.

Regulations

Ireland

Data privacy. The EU's Data Protection Commission (DPC) announced a final decision on an investigation into TikTok, fining the video and social media company €530 million (\$597.7 million) for the transfer of EU users' data to China.

After a four-year investigation, the commission determined at the beginning of May that TikTok had breached EU data privacy rules under the General Data Protection Regulation (GDPR) and placed users at risk of surveillance.

The DPC found that the company failed to properly inform users about which nations, including China, that personal data was transferred to. "TikTok's personal data transfers to China infringed the GDPR because TikTok failed to verify, guarantee, and demonstrate that the personal data of [EU] users, remotely accessed by staff in China, was afforded a level of protection essentially equivalent to that guaranteed within the EU," said DPC Deputy Commissioner Graham Doyle in a statement.

Along with the monetary fine, the DPC ordered the company to comply with GDPR rules within six months.

South Korea

Aviation safety. The Ministry of Land, Infrastructure, and Transport ordered

that all 15 airports in South Korea install bird detection cameras and thermal imaging radars.

The additional technology should help in spotting birds so pilots can avoid collisions.

The new rule was issued after an investigation into the deadliest plane crash recorded on South Korean soil. Investigators of the December 2024 Jeju Air Flight 7C3316 crash at Muan International Airport found feathers and blood stains on the plane's engines, indicating bird strikes played a role in the crash that resulted in 179 deaths.

U.S. States

Cybersecurity. New York state will subject water and wastewater utilities to stricter cybersecurity standards.

The new regulations require water and wastewater providers in the state with more than 3,300 customers to obey cybersecurity measures. These include performing an annual cybersecurity vulnerability analysis, creating and implementing formal cybersecurity programs and incident response plans, training staff on cybersecurity hygiene, and adhering to new incident reporting requirements. Additionally, regulated entities will be required to develop and maintain response and recovery plans to support continuity of operations in the event of cyberattacks.

For larger utilities—ones with more than 50,000 customers—there will be an additional requirement of designating an employee responsible for managing a cy-

bersecurity program, as well as monitoring and recording network activity.

Members of the state's environmental conservation, health, and public service departments developed the regulations. Utility providers will also have access to a newly created \$2.5 million grant program to assist with the costs of the regulations.

"Cyberattacks on critical infrastructure can have devastating impacts on communities, and we must act now to defend our water and wastewater systems with the same urgency and rigor we bring to other critical sectors," said New York Governor Kathy Hochul in a press release. "These new regulations and grant programs reflect our commitment to protecting public health and safety while helping under-resourced entities modernize for a digital age." ■

ADVERTISERS INDEX

Please visit our *Security Management* advertisers at GSX in New Orleans, Louisiana.

BOOTH #	PAGE NUMBER
1627	Allied Universal 11
2155	Altronix 28-29
1455	Ameristar Perimeter Security 17
1327	AXIS Communications 04
2361	Axon Enterprise Partial Tip-on
2243	CEIA USA 13
2326	Hanwha Vision 06
2508	Impact Security, LLC 57
-----	Ionodes 47, 53, 59, 65
519	Liferaft 67
3713	Morse Watchman, Inc. 34-35
2527	Napco Security Technologies 68
2527	Napco Security Technologies S2, S24
2314	Par-Kut International 23
1927	Securitas Technology 08
736	Splan 30
-----	StrongPoles 38
1419	Safety Technology International (STI) 22
-----	Titan 41
3113	Verkada 54-55
-----	VonLoewenfeldt Group 31
1277	Zbeta BB, 2-3

EXHIBITOR MAP SPONSORS:

1339	Wallace Perimeter Security S10-11
1927	Securitas Security Services, USA S10-11
2527	Napco Security S10-11
2938	International SOS S10-11

Allied Universal
aus.com

Altronix
altronix.com

Ameristar Perimeter Security
ameristarperimeter.com

AXIS Communications
axis.com

Axon
axon.com

CEIA
ceia.net

Hanwha Vision
hanwhavisionamerica.com

International SOS
internationalsos.com

Impact Security
defenselite.com

Ionodes
ionoeds.com

Liferaft
liferaftlabs.com

Morse Watchman
morsewatchmans.com

Napco Security Technologies
napcosecurity.com

Par-Kut International
guard-booth.net

Securitas Technology
securitastechnology.com

Splan
splan.com

StrongPoles
strongpoles.com

Safety Technologies
sti-usa.com

Titan
tpcsecurity.com

Verkada
verkada.com

VonLoewenfeldt Group
teamsoftware.com

Wallace Perimeter Security
wallaceperimetersecurity.com

ZBeta
zbeta.com

CLOSING SCHOOL EMERGENCY ALERT GAPS FOR FIRST RESPONDERS

Edge computing cameras manufacturer i-PRO Americas, Inc., announced a strategic partnership with NovoTrax, an end-to-end life safety and mass notification company. The partnership will blend the companies' respective strengths with the goal of eliminating long-standing integration gaps between video security and mass notification systems—gaps that can waste crucial time during emergency events. The partnership aims to provide first responders with immediate, actionable intelligence, including live video, real-time location data, and integrated communications, within seconds of an emergency alert being triggered.

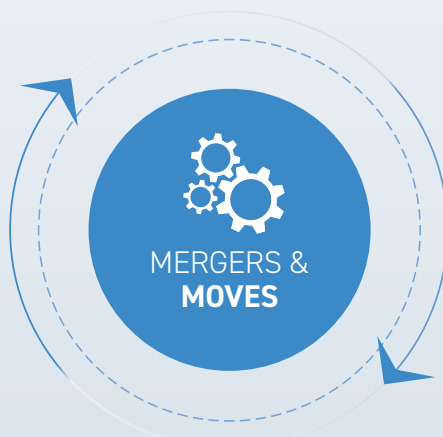


HID ⇄ Calmell Group

Identity solution provider HID announced the acquisition of Calmell Group, a Spanish manufacturer of smart cards, smart paper tickets, and magnetic tickets.

Allegion plc ⇄ Summit Partners

Through one of its subsidiaries, Allegion acquired ELATEC, including Elatec GmbH and other entities, from Summit Partners for €330 million (\$383.7 million).



Triton ⇄ Bosch

Triton purchased Bosch's security and communications technology product business, which includes video systems, access control, and intrusion alarm systems.

Honeywell ⇄ Li-ion Tamer

Honeywell's acquisition of Li-ion Tamer deepens the company's portfolio of fire and life safety technologies.



Award

HID and ASSA ABLOY's BG100 Speedgate won a 2025 Red Dot Award for product design in the interior design elements category.



Contract

The U.S. Department of Defense's Data Readiness for Artificial Intelligence Development awarded Agile Defense a two-year \$35 million contract to advance data readiness in support of artificial intelligence operations.



Announcement

The Canadian government ordered Chinese surveillance camera manufacturer Hikvision to stop operating in Canada due to national security concerns. Hikvision challenged the order.

Partnerships



Retail Surveillance

The Mall of America announced it is expanding its partnership with Axis Communications by implementing car-counting video analytics.

Public Safety

ProLogic ITS announced a partnership with Signal 8. Together they will highlight Signal 8's software platform, Smart Squad, which offers tools that can improve officer safety and operational efficiency.

Safer Roads

Verra Mobility Corporation, which provides smart mobility technology solutions, announced a partnership with California's Oakland City Council.

THE OPEN-PLATFORM SOLUTION TO UNIFY YOUR VIDEO SYSTEMS, WITH INSIGHTS.



UNLOCK THE FULL POTENTIAL OF YOUR VIDEO SYSTEMS.

Share live and recorded video from remote sites with a centralized system while leveraging business intelligence, automatic person of interest detection and real-time alerting. Integrated with Genetec and Milestone.



Start your
journey today.

IO NODES  verifyfaces.com



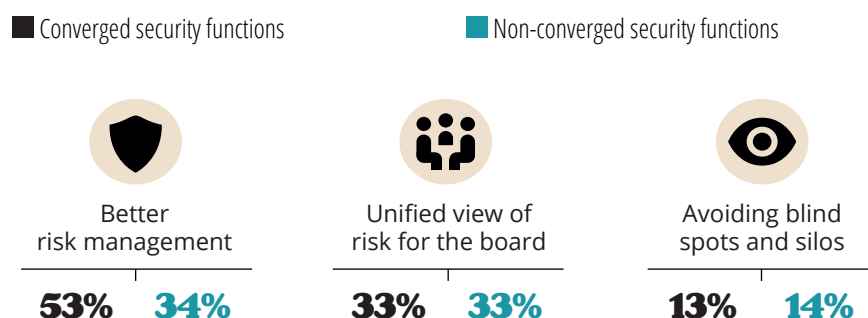
Success Factors for Holistic Security

- Identity and culture.**
Clear rationale for partnership
- Leadership.**
CSOs and CISOs working across silos
- Incentives.**
Clear motivation to collaborate
- Clarity of roles.**
Formally documented roles and responsibilities
- Professional development.**
Cross-function learning
- Shared reporting.**
Joint reporting to enhance problem-solving
- Operational.**
Joint working groups and shared personnel
- Governance.**
Present a holistic picture of risk

Instead of Convergence, Prioritize Partnerships

Only 15 percent of organizations have integrated their corporate and cybersecurity teams; for most, it's not in the cards. Recent research from The Clarity Factory, *Holistic Security: How physical and cyber security can join forces to strengthen operational resilience*, recommends pursuing cross-organizational partnerships and resource-sharing through a holistic security model instead. Those partnerships can improve security outcomes, especially as risks are increasingly intertwined between physical and cyber teams.

What's the top benefit to collaboration between corporate/physical and cybersecurity?



What's the biggest obstacle to CSOs running cross-security collaboration?



Your Threat Intelligence Partner.

Detect • Alert • Act • Prevent



The best way to protect your people, assets, brand, and data is to know what's coming.

Liferaft cuts through online noise to identify and validate threats across the broadest range of mainstream and niche open source channels available online. We help companies protect people, assets, and businesses, making the world around us safer every day.



Get to know Liferaft iQ

Liferaft iQ transforms the overwhelming into the actionable, by processing vast volumes of open-source intelligence and delivering high-context insights that support faster, more confident decisions.

Save critical time by automating the collection of:

- Social Media
- Deep web pages
- Darknet sources

Advanced filtering with:

- Customized search criteria
- Geofences, mapping assets, and safety scoring
- Curated intelligence feed
- POI insights



We're here to help.

Drop by **Booth 519** to find out how Liferaft can support your security initiatives.

liferaft

liferaftlabs.com



NAPCO SECURITY

Share Tech
& Drinks
With Us
Booth
2527

 **More Security**

 **Smarter Tech**

 **Less OpEx**

Today's Smart Solutions. Dependably Made Under One Roof

Napco Security Technologies has been designing & manufacturing the security, fire, access control & locking systems, that businesses, schools, residential properties, institutions, and government have come to rely on for over 50 years. While times and technologies change, the commitment and adherence to the highest industry standards for quality, durability, & customer care should not. Know, that although we make natively integrated hardware and software solutions for every security application & budget, our entire company is dedicated to just one thing: *Keeping yours secure.*



GSX Booth 2527: Join us for Demos & Drinks Mon. & Tues. 3-4:30pm, Daily Prize Giveaways



Access

Fire

Intrusion

Locking



 **NAPCO**
SECURITY TECHNOLOGIES, INC.

1.800.645.9445 • www.napcosecurity.com
Amityville, NY USA • NASDAQ:NSSC