SECURITY MANAGEMENT

Published by ASIS International
September 2024

The Art of Concierge Guarding

When debating security policies, procedures, and technologies, don't overlook the value of positive human connection. **By Sara Mosqueda**

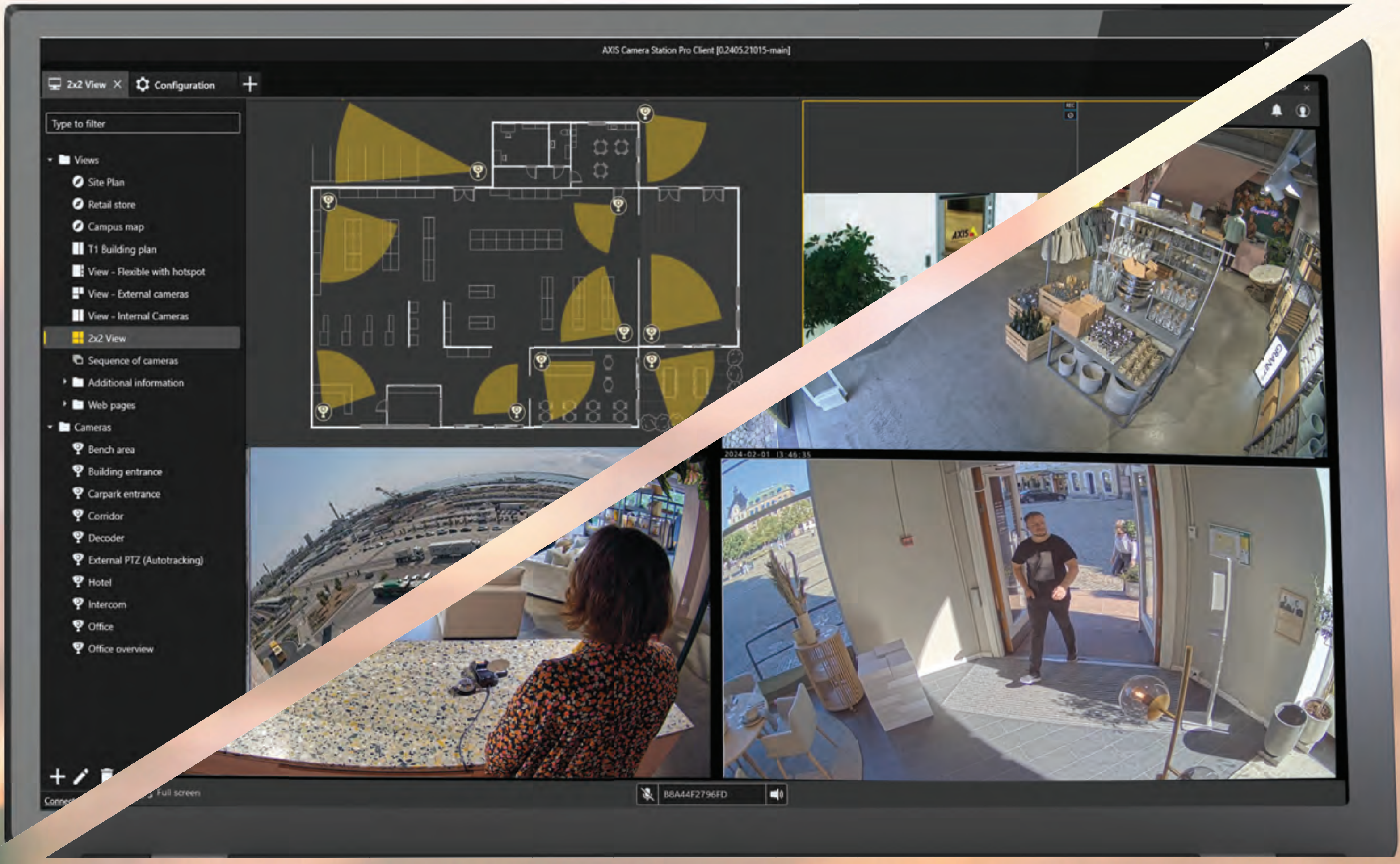
AXIS COMMUNICATIONS

AXIS Camera Station

Two VMS options, unlimited possibilities

AXIS Camera Station Pro

Server-based video and access control management with cloud capabilities.



AXIS Camera Station Edge

Cam-to-cloud video management leveraging Axis edge devices.

See us at GSX Booth 1414

ASIS FOUNDATION™

Thank You to Our **Sponsors!**

Your Support Fueled Our Fitness Challenge Success—Together, We Made Every Step Count!

DSS
DOYLE SECURITY SERVICES

THERMAL™ RADAR
Visionary Thermal Detection

SAGE integration
EMPOWERED INSIGHT. PROTECTED FUTURES.

stapp one

Hanwha Vision

AI powered.
Cloud connected.

OnCloud

Manage resources across multiple sites with OnCloud, a direct-to-cloud video management system. Experience low-latency access to live and recorded video, view searchable clips, receive event notifications and more.

DMPro

Ensure your cameras are up-to-date and secure with DMPro, a cloud-based solution for device maintenance and total system health monitoring.

SightMind

Harness the data and gain insights into your operations with AI metadata visualization software from Hanwha Vision.

FLEX AI

Expand beyond the limits of people and vehicle detection by training your cameras for custom object detection – using as few as 20 images.

GSX
GLOBAL SECURITY EXCHANGE
BOOTH #1701

Contents Notable

"It turns out threats to kill are very, very common in elementary school, and they're overreactions."

Dr. Dewey Cornell explains how behavioral threat assessment in K-12 schools needs to take childhood development into consideration. **Page 38**

300%

Potential turnover rates among security guard forces, putting a spotlight on workplace culture as a reason to leave.
Page 54

"Adversaries could also employ insiders to assist with their malign influence operations to undermine American confidence in the security and integrity of the elections process."

New guidance seeks to mitigate insider threats to the American electoral system. **Page 26**

"The word 'effective' to me may mean something different to you."

Steve Powers examines the unknowns in a new California workplace violence prevention plan law.
Page 15

28 sq ft.

The amount of space a specialized safety shelter takes up in K-12 classrooms, providing a haven during emergencies.
Page 23

67

The percentage of CSOs who said customer service skills were extremely important in frontline security employees, according to a 2023 report.
Page 30

Security Management Volume 68, Number 2, is published twice a year and distributed at various industry tradeshows by ASIS International, 1625 Prince St., Alexandria, VA 22314; 703.519.6200; fax: 703.519.6299. Single copies are available for purchase at *store.asisonline.org*. *Security Management* is a registered trademark, and its use is prohibited. Statements of fact and opinion are made on the responsibility of the authors and do not imply an opinion on the part of the editors, officers, or members of ASIS. Advertising in this publication does not imply endorsement or approval by *Security Management* or ASIS. The editors reserve the right to accept or reject any article or advertisement. Quantity reprints of 100 or more copies of each article may be requested from *Security Management* Reprints Dept. by contacting *keith.schilling@asisonine.org*.

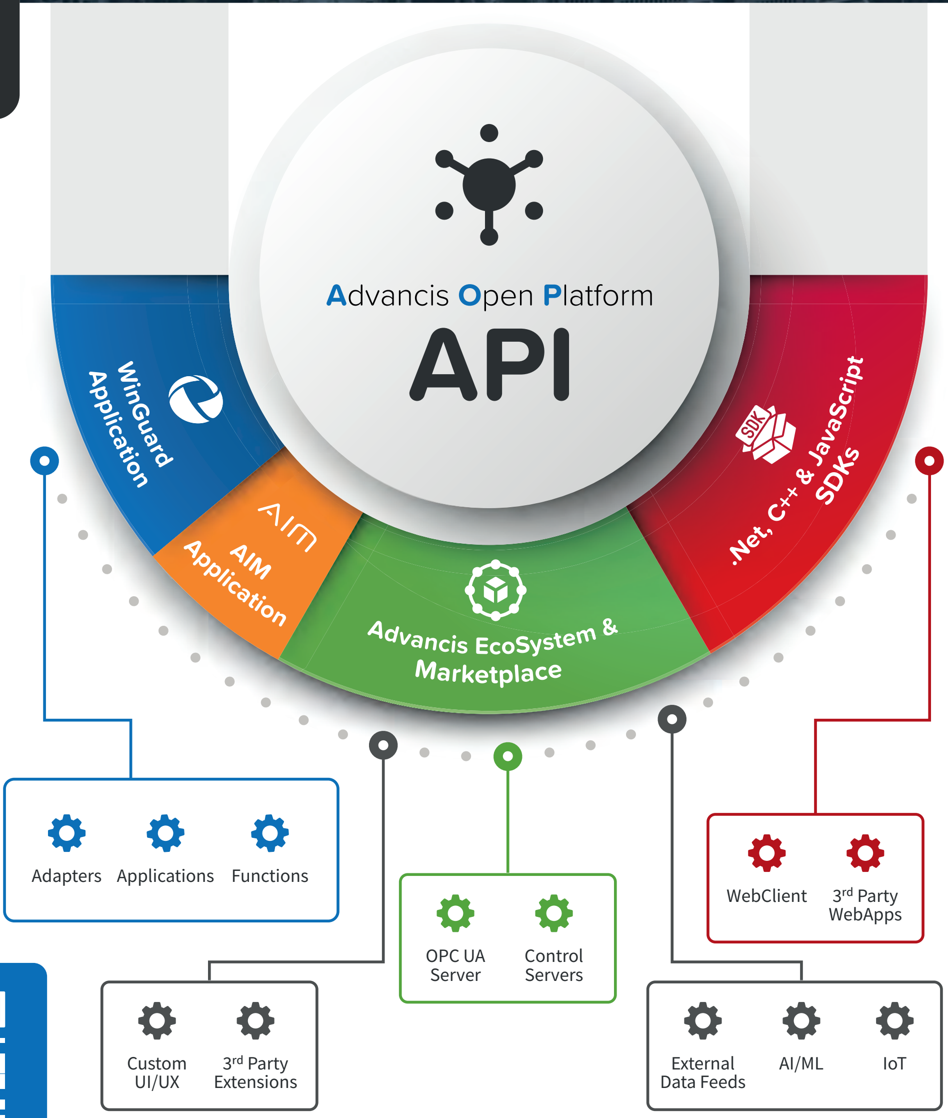
Voting and handshake photos by iStock; classroom photo courtesy of Quitman School District

INTRODUCING ADVANCIS OPEN PLATFORM (AOP)

The software platform every **integrator** has been waiting for.

Have you been searching for a new **software platform** that allows you to create **customer-specific** applications?

The wait is over.
AOP is here.



See us at GSX Booth 1938

advancis

For more information visit **advancis.net**
or contact us at **usasales@advancis.net**

Contents Features

SEPTEMBER 2024

EXECUTIVE TEAM

William W. Tenney
chief executive officer
William.Tenney@asisonline.org

Christine M. Peck, CAE
chief global learning officer
Christine.Peck@asisonline.org

Teresa Anderson, CAE
vp, innovation and outreach
Teresa.Anderson@asisonline.org

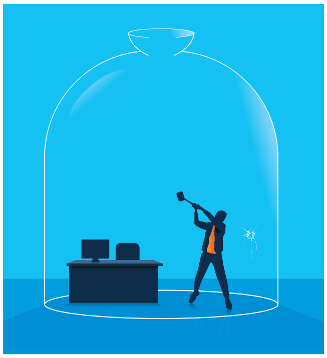
Nello Caramat
publisher
Nello.Caramat@asisonline.org

ASIS INTERNATIONAL
1625 Prince Street
Alexandria, VA 22314
703.519.6200
fax 703.519.6299

MEDIA SALES

Charlotte Lane
Account Manager
Companies # through L
703.518.1510
Charlotte.Lane@asisonline.org

Femke Di Cesare
Account Manager
Companies M through Z
703.518.1502
Femke.DiCesare@asisonline.org



Cover illustration by Taylor Callery

KeyWatcher TOUCH
KeyWatcher TOUCH

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

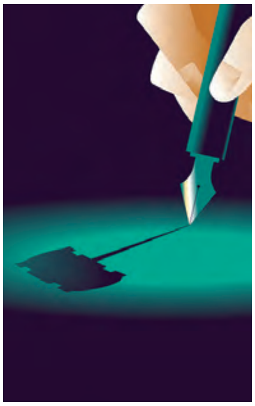
Mariah Bartz
associate art director
Mariah.Bartz@asisonline.org

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.



Contributing Authors

Sarah J. Powell

FOUNDER
SP2 STRATEGIES

Sarah J. Powell has spent more than 20 years in the risk and resilience space as a researcher, practitioner, and leader. She continues to be focused on building the resilience of individuals, teams, and organizations on a local and global scale, even when that means transforming existing cultures. Powell is currently the deputy chief transformation officer for safety culture at the Southeastern Pennsylvania Transit Authority, and she is also the founder of consulting enterprise, SP2 Strategies.

"Escape from Toxicity," Page 52

Theodore P. Barron, CPP

Theodore P. Barron, CPP, is the former chair of the ASIS Bay Area Chapter San Francisco, California. He is also a former vice president of security at Wells Fargo Bank where he was responsible for the development and management of key physical security programs within the corporate security department.

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. He has more than 20 years of industry experience in information systems security and privacy. His areas of expertise are in risk management and mitigation, security and privacy regulatory issues, design and implementation of systems security, encryption, cryptography, and security policy development. He wrote *Computer Security—20 Things Every Employee Should Know.*

Book Review, Page 25

SecureStat HQ™

Clarity and Control to Optimize Your Security.

Take the complexity out of security management with SecureStat HQ™. It's an enterprise-grade digital platform that gives you visibility and control of sites, systems, and users. It both streamlines day-to-day tasks and drives consistency in procedures and reporting across your organization – with insight on how to improve. Best of all, it's your gateway to our award-winning services: installation, maintenance, monitoring, lifecycle management and more. Discover more at **securitastechnology.com**.

Securitas
Technology

See us at GSX Booth 1400

See a different world.

NUANCED COMMUNICATION

A failure to communicate can often be traced to simple misunderstandings. For example, people do not understand that there is a "difference between Chinese characters and Chinese languages," according to Mark Swofford, a scholar of pinyin—the practice of writing Chinese words using the Roman alphabet.

Swofford, quoted in a *Chicago Tribune* article on the subject, said this confusion can lead to significant problems. For instance, there is an oft-cited claim that the Chinese character for "crisis" is created by combining the characters for "danger" and "opportunity."

Although this concept is attractive, it is quite incorrect. It is a misunderstanding of how words are formed in Mandarin and other similar languages. The word for crisis, pronounced "weiji," is indeed made up of two characters. One part of the word ("wei") means danger, but the other ("ji") translates to something like "a crucial point when something begins or changes." So, the meaning of the word is similar to the English definition of a crisis—a turning point or a condition of instability or danger.

Teresa Anderson

Claire Meyer

Of course, security professionals have a much more nuanced understanding of the word "crisis," and they understand that opportunity comes in preparing to meet crises. They strive to assess what a crisis is, when it will come, and how it will manifest.

With hundreds of education sessions and learning opportunities, as well as an exhibit hall packed with the latest in products and services, GSX 2024 is the perfect place to learn how best to meet a crisis. This special issue of *Security Management* is crafted to help frame your mindset at the event and beyond.

Words matter—both in definition and context. Our September issue exemplifies how great communication among industry peers helps everyone do the work of making the world safer. Learn from museum security experts about how a concierge approach smooths interactions with protesters, study how to de-escalate students in crisis, and practice advocating for yourself and your team when facing toxic conditions.

As you read these articles, note how having a stellar communicator on your team can make all the difference, even in the absence of a crisis—lessons applicable to our own *Security Management* team.

After more than 30 years at the publication and a decade as editor-in-chief, I will be stepping into a different role—promoting partnerships and developing new products and services at ASIS.

Meanwhile, the *Security Management* team will continue its legacy of nuanced communication and reporting under a new leader and editor-in chief. Claire Meyer will bring her 15 years of experience writing about the security industry as she moves from managing editor to editor-in-chief of *Security Management*. She will be an excellent steward of the security industry's premier publication, helping professionals prepare for crises and embrace opportunity. ■

Teresa Anderson
Editor-in-Chief, 2013-2024

Teresa Anderson

Claire Meyer
Editor-in-Chief, 2024-

Claire Meyer

Illustration by iStock

fire & emergency
communications power
access control &
power integration
network power
management
ARENA
BANK
BAGELS
PIZZA
MARKET
surveillance
power & data

Great Expectations

California's Senate Bill 553 requires nearly all employers with a workforce in the U.S. state to create, adopt, and implement written workplace violence prevention plans.

By Claire Meyer

California's Senate Bill 553 (SB 553) is now in effect, requiring nearly all California employers to create, adopt, and implement written workplace violence prevention plans.

The law amended the U.S. state's labor and civil procedure codes to require most organizations to establish a written workplace violence prevention plan and employee training program by 1 July 2024. There are a few exempt organizations, including employers covered by existing workplace violence prevention in healthcare standards and locations not open to the public with fewer than 10 employees.

SB 553 does a very good job of calling out the violent incident log and having data to be able to drive mitigation and correction.

The law is enforceable under California's division of the Occupational Health and Safety Administration (Cal/OSHA). But it's unclear at the moment what enforcement will look like, how regulators will assess unique cases, and what will be deemed "effective" measures under the law, says Steve Powers, associate managing director of the enterprise security risk management practice at risk and financial advisory firm Kroll.

"The word 'effective' is referenced in the bill several times, but what does the word effective mean?" he asks. "Is that zero incidents? Which is an unrealistic mea-

Illustration by iStock; *Security Management*

sure. But no one has defined what effective means. So, if somebody comes in and Cal/OSHA inspects my particular business and says, 'Your plan is ineffective,' I would hope they spell out what they mean by that. The word 'effective' to me may mean something different to you."

Despite those unknowns, Powers says that SB 553 is one of the most comprehensive pieces of workplace violence prevention law he has seen, expanding the focus across industries and addressing best practices and prevention.

In general, workplace violence legislation is brought about as a response to an incident, and SB 553 is no exception. It was originally prompted by the 2021 shooting at the Valley Transportation Authority railyard in San Jose, California. The bill was pushed forward amid increases in workplace assaults and violence during the COVID-19 pandemic before being passed in October 2023.

Cal/OSHA had been developing a Workplace Violence General Industry plan for years, and SB 553 accelerated the creation of the standard. The plan is due to be adopted by no later than 31 December 2026. But in the meantime, employers must still create workplace violence prevention programs, even though the parameters can feel a little fuzzy.

"SB 553 goes into effect during a time of heightened risk," wrote *Insurance Journal.* "Political violence in the U.S. is at its highest point since the 1970s, and this year's presidential election could trigger further violence. It is certainly an opportune time for businesses to acknowledge and prepare for the potential for violence in the workplace. But despite placing a clear responsibility on employers to develop these plans, the bill stops short of detailing what the plans should look like, and many businesses may find themselves unprepared as a result."

Personally, Powers says that many businesses are not ready for this moment.

"I also assume that Cal/OSHA is not equipped to begin immediate inspections and would likely do so in response to an incident," Powers explains.

"This particular bill is very robust. It attempts to address workplace violence from every perspective, except maybe threat assessment and management," he adds. "It does a very good job of calling out the violent incident log and having data to be able to drive mitigation and correction."

What Does SB 553 Cover?

The law requires businesses—including those not based in California but with an employee presence in the state—to address all four major types of workplace violence in their plans and training.

Type 1: criminal intent. Workplace violence committed by a person who has no legitimate business at a worksite, including retail robberies, robberies of cab drivers, and threats and acts of violence directed at security guards.

Type 2: customer/client. Workplace violence directed at employees by customers, clients, patients, students, inmates, or visitors.

Type 3: worker-on-worker. Violence against an employee by a current or former employee, supervisor, or manager.

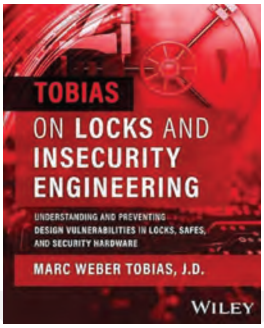
Type 4: personal relationship. Violence committed in the workplace by a person

Book Review

Tobias on Locks and Insecurity Engineering

By Marc W. Tobias, JD. Wiley; www.wiley.com; 720 pages; $80.

Tobias on Locks and Insecurity Engineering: Understanding and Preventing Designing Vulnerabilities in Locks, Safes, and Security Hardware by Marc W. Tobias offers insights and understanding of design vulnerabilities in locks, safes, and security hardware. While the book is directed toward engineers involved in lock and key system design, it emphasizes the importance of acknowledging the existence of potential vulnerabilities within any security design. The book provides suggested criteria for a proactive approach to identify and mitigate the risk of failure for these devices.



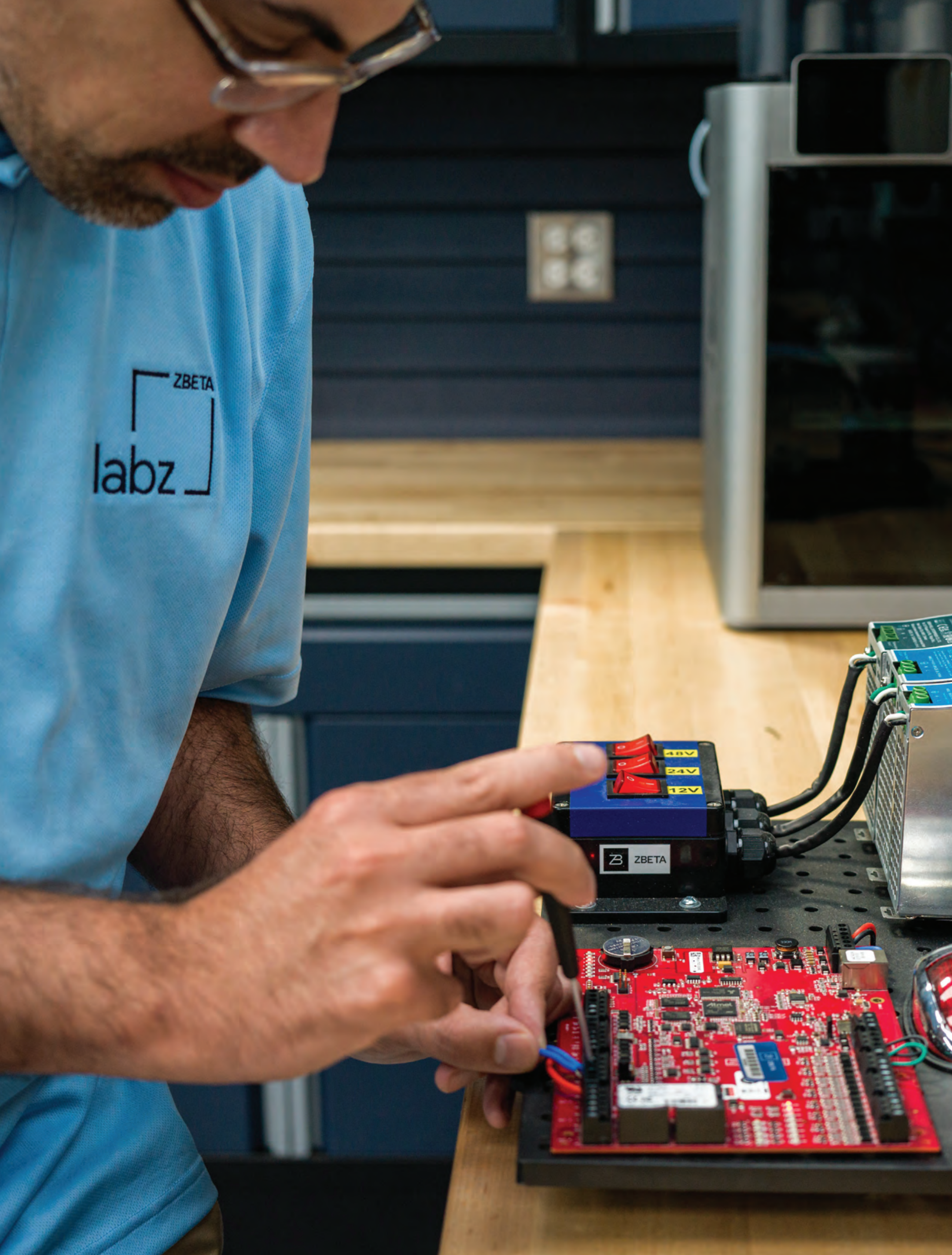
The book serves as a comprehensive engineering reference, delving into both mechanical and digital aspects of lock science. With meticulous organization and well-indexed content spanning approximately 700 pages, Tobias ensures accessibility for readers navigating the complexities of security hardware design.

Drawing from his expertise in liability law, Tobias provides valuable insights into the consequences and costs associated with design flaws. Through detailed analysis, he states the origins of these flaws and advocates for a management and engineering culture that prioritizes resilience in risk strategy and forward thinking on design.

While providing technical details on its primary subject, the book also offers compelling arguments that underscore the importance of addressing security vulnerabilities through every phase of design. Tobias's law enforcement field operations and legal perspective add depth to the discussion, highlighting the implications of negligence in design and the imperative for proactive risk management.

Overall, this book offers a straightforward and level examination of security engineering principles, while urging practitioners to adopt a vigilant mindset and embrace continuous improvement in their designs. The book provides an excellent resource for engineers, management professionals, and law enforcement who are tasked with safeguarding against the ever-present threats to the multiple arrays of security systems we now employ to safeguard ourselves and our companies.

Reviewer: Theodore P. Barron, CPP, is the former chair of the ASIS Bay Area Chapter San Francisco, California. He is also a former vice president of security at Wells Fargo Bank where he was responsible for the development and management of key physical security programs within the corporate security department.


ZBETA
labz
48V
24V
12V
ZBETA

who does not work there but has, or had, a personal relationship with an employee.

Workplace violence can entail any act or threat in the form of physical aggression, harassment, intimidation, or threatening behavior at a workplace.

The law requires employers to log violent incidents and provide training on workplace prevention, including additional training when new hazards are identified or the plan changes.

One challenge is that hazards are not clearly defined in the law. The term workplace hazard is most regularly used with workplace safety measures like spills, chemical access, or fall risks, but it is being articulated differently in SB 553, Powers says. In this case, a workplace violence hazard could potentially include circumventing security procedures, such as propping open a door for a smoke break or sharing credentials. The location of the business itself or the type of operation it's engaged in could also be considered hazards that need to be addressed with a plan.

Workplace Violence Prevention Plan Requirements

Employers need to start with an assessment to identify and evaluate workplace violence hazards. These could include the exchange of money, lone workers, working at night, availability of valuable items, performing public safety functions in the community, or working with people or customers who have a history of violence or threatening behavior.

The plan can be incorporated into a company's injury and illness prevention program, it must be in writing, and it must include:

- Names or job titles of the people responsible for implementing the plan
- Effective procedures to obtain active involvement from employees and their representatives in developing and implementing the plan—including in identifying hazards, designing training, and reporting incidents
- Methods the employer will use to coordinate plan implementation and ensure employees know their roles in the plan
- Effective procedures for the employer to accept and respond to reports of workplace violence, prohibiting retaliation against employees who report hazards
- Effective procedures to communicate with employees about workplace violence matters
- Effective procedures to respond to actual or potential workplace violence emergencies
- Procedures for post-incident response and investigation
- Procedures to review and revise the plan as needed

Plans must be reviewed at least annually. They must also be reviewed and revised any time a deficiency or new hazard

is observed or reported, or after a workplace violence incident occurs.

These workplace violence prevention plans require employee input, seeking to alter the typical top-down policies to have more real-world applications and feedback. The law does not specify, however, exactly how much employee input is needed to fulfill that requirement.

California's Department of Industrial Relations developed a model workplace violence prevention plan as a starting point for employers, but plans must be customized to address specific workplace needs—a basic template will not fulfill regulatory requirements. The plan needs to be a living document that evolves based on changing hazards and employee input, Powers says.

In some cases, organizations might need more than one plan. According to a Global Guardian interview with Robin Welch Stearns of the Pacific Resilience Group, a pharmaceutical company with manufacturing facilities and offices in California will likely need two plans—one for each type of site and its unique hazards.

Training Requirements

SB 553 requires employers to provide initial training when the plan is established and provide annual training thereafter. Training must use appropriate content and vocabulary for the educational level, literacy, and language of employees, according to a briefing by law firm Procopio, Cory, Hargreaves, & Savitch LLP.

The training cannot be an off-the-shelf security awareness or workplace violence training. It must be designed based on the specific elements of the employer's written workplace violence prevention plan.

Training needs to include:

- The employer's workplace violence prevention plan and how employees can obtain a free copy of the plan
- How to report workplace violence hazards and incidents
- Corrective measures that the employer has taken on workplace violence hazards
- How to seek assistance to prevent or respond to violence
- Strategies to avoid physical harm
- Information about the violent incident log and how employees can obtain a copy

Employers must retain training records for at least one year.

Reporting Requirements

Employers are required to keep detailed logs of workplace violence incidents that can be made accessible to employees and others, but without personally identifying information. That log must include:

- Data, time, and location of an incident
- Detailed description of the incident
- Classification of who committed the violence (stranger, customer, worker, or domestic partner)
- Violence type, such as physical attack or threat, whether weapons were involved, or if it was a sexual assault
- Consequences of the incident, such as whether security or law enforcement was contacted

This log must be retained for five years. Employees can request to view and copy the log, which must be provided within 15 calendar days of the request.

Changes to Restraining Orders

SB 553 also enables employers to petition for temporary restraining orders (TRO) and orders after hearings on behalf of employees.

SB 553 "authorizes collective bargaining representatives, not just employers, to petition for TROs on behalf of employees, allowing even more relief for employees faced with threats and violence," explained law firm Seyfarth in a summary of the California law. "SB 553 also provides for employee names to be withheld from the TRO papers, providing anonymity for victims who otherwise might have hesitated on supporting a TRO for fear of retaliation from the individual at issue."

The new law also expands which types of conduct qualify for a TRO and allows employers to seek orders on behalf of employees who suffer harassment, not just violence or threats of violence.

Key Elements Remain Ambiguous

There are still a lot of questions around the implementation of this law, including what enforcement looks like and what counts as "effective." Civil penalties and fines are on the table, but will Cal/OSHA conduct inspections or will those penalties be levied after an incident?

Fines for Cal/OSHA violations can be steep—up to $15,000 for general or regulatory violations and nearing $159,000 for willful and repeat violations. Non-compliance can also put organizations at risk for increased litigation. So, it behooves organizations to make a good faith effort at compliance while waiting for the regulatory equivalent of case law to set precedents on what counts and what doesn't under the new law, Powers says.

Along with their employees, employers should consider contractors or other third-party individuals: Whose responsibility is it to ensure they know an organization's plan? Would they be able to request access to the organization's log of incidents?

Even which businesses are exempt from the law can be debated. For organizations with a small office of nine employees in California, they could be exempt provided there is no public access to the office.

But how far does "no public access" reach, Powers asks. What if the office accepts deliveries or has a team meal catered? What if unexpected visitors or customers come to the office to seek a meeting? For a law office, would runners bringing court documentation count as public access? Is total isolation required to meet that exemption? How would this rule apply to remote workers who gather occasionally for team meetings or outings?

In addition, Cal/OSHA has the right to overrule an exception, but it is unclear when that would apply. It is likely that the regulator could reassess a business's exempt status after an incident and make it subject to the law moving forward, Powers says.

"I would hope that Cal/OSHA is going to provide some updated guidance because people are just throwing things out there," he adds. "There's a lot of confusion."

The law could also place a significant burden on employers, especially small businesses with limited resources and staff time. Powers references the idea of a family-owned convenience store, which is open to the public, open during late hours, and could face criminal activity and violence. That business would need to establish a workplace violence prevention plan and train staff on it. Then, with each subsequent hazard identified or incident—including attempted robberies or harassment—the business would need to reassess its hazards, mitigate, and retrain.

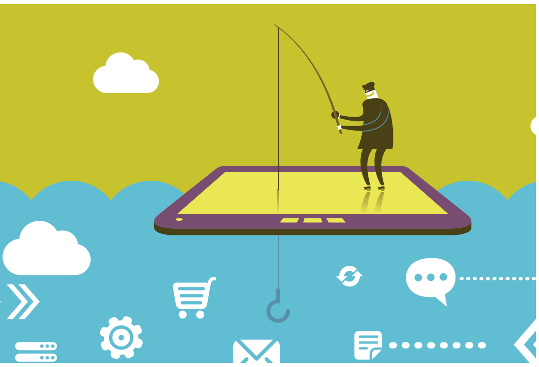
"Depending on the size on of an organization, this is going to require a tremendous amount of input and time, and for entities without a security organization or dedicated environmental health and safety office, they don't have the ability to do this, and they are scrambling," Powers says.

Even businesses without a presence in California should pay close attention to this rollout.

"While California is the first state to enact such a broad workplace violence prevention law, other states are considering similar legislation," *Insurance Journal* explained. "There were more than 100 workplace violence bills introduced last year across 27 states, with a quarter of those bills enacted and half still pending, according to LexisNexis State Net Insights. Employers in all those states should also be watching the rollout of SB 553 closely, as they may soon find themselves with similar requirements."

Powers adds that "there's a lot to unpack with this. I think they're trying to do the right thing, but this is far easier said than done."

Fooled by Fake Tech Support



Don't trust unsolicited tech support. According to a May 2024 data spotlight from the U.S. Federal Trade Commission (FTC), consumers reported 52,000 instances of scammers impersonating Best Buy or its Geek Squad tech support brand in 2023, far more than the second most-impersonated brand, Amazon (34,000 reports).

In 2023, the FTC tallied more than 330,000 reports of business impersonation scams and nearly 160,000 reports of government impersonation scams—nearly half of the fraud reported directly to the FTC by consumers last year—with combined reported losses of $1.1 billion.

Consumers didn't lose the most money to Geek Squad impersonators, though. That honor went to scammers pretending to be Microsoft, with $60 million lost (7,000 reported scam attempts), followed by Publishers Clearing House at $49 million (also 7,000 reported scam attempts).

"The scammers impersonating these businesses work in very different ways," the FTC spotlight explained. "For example, phony Geek Squad emails tell you that a computer service you never signed up for is about to renew—to the tune of several hundred dollars. Microsoft impersonation scams start with a fake security pop-up warning on your computer with a number to call for 'help.' And calls from the fake Publishers Clearing House say you'll have to pay fees to collect your (fake) sweepstakes winnings."

The top five impersonation fraud scams identified by the FTC are:

Copycat account security alerts. These scams send victims messages about alleged suspicious activity or unauthorized charges and get directions on how to fix the fake problem, often by transferring funds.

Phone subscription renewal scams. These alert the victim that an account they never opened is about to auto-renew.

"If you call to sort it out, they'll say they have to connect to your computer to process your 'refund,'" the FTC explained. "Once in, they make it look like too much money was refunded. They demand that you return the difference, often by buying gift cards and giving them the numbers on the back."

Fake giveaways, discounts, or money to claim. These messages all serve as setups, grabbing the victim's attention before convincing them to send money or gift cards to claim the deal or gift.

Bogus problems with the law. Calls or messages claiming the victim is involved in a crime—especially money laundering or drug smuggling claims—enable scammers to offer to help victims fix the problem by telling you to move money or put it on gift cards to protect it during the fake investigation.

Made-up package delivery problems. These frequently involve texts from the U.S. Postal Service, claiming there is a problem with delivery and providing a link to a website that looks real to help resolve it. Some ask for bank account details or ask you to pay a small "redelivery fee." This gives the scammer the victim's credit card information, which they quickly use to rack up fraudulent charges.

"All these scams have tactics that scammers hope give them an advantage," the FTC said. "First, their messages look a lot like the messages real companies send: emails or texts about special deals and security alerts on your accounts. Second, they play on your emotions: if you're worried about a problem or excited about a free gift, it can be harder to spot signs of a scam. Finally, they reframe their demands for money to avoid setting off alarm bells: people who'd never send money to a stranger have emptied their accounts, believing they were 'protecting' their funds."

Scammers are also blurring the lines between fraud types, often impersonating more than one organization in a single scam attempt, like a fake Amazon employee transferring a victim to a fake bank or fake FBI employee, the FTC said.

Fraudsters reached out most often by email and phone calls, but people lost the most money on scams that originated on social media—especially online shopping scams that started with ads on Facebook and Instagram. Investment scams—like pig butchering schemes—on social media led to the largest reported losses.

Scammers requested a variety of payment methods, especially cryptocurrency and bank transfers. Gift cards were also frequently used, especially for romance scams, tech support scams, government impersonation scams, and scams that impersonate people you know, like a boss or relative. Scammers will often specify which gift card brand to buy, preferring Apple gift cards (30 percent), followed by Target (14 percent) and eBay (9 percent).

The report came shortly after a new FTC rule became effective, giving the agency stronger tools to address and deter scammers who impersonate government agencies and businesses. This includes enabling the FTC to file federal court cases to try and get money back to victims and seek civil penalties against rule violators. ■

Illustration by iStock; *Security Management*

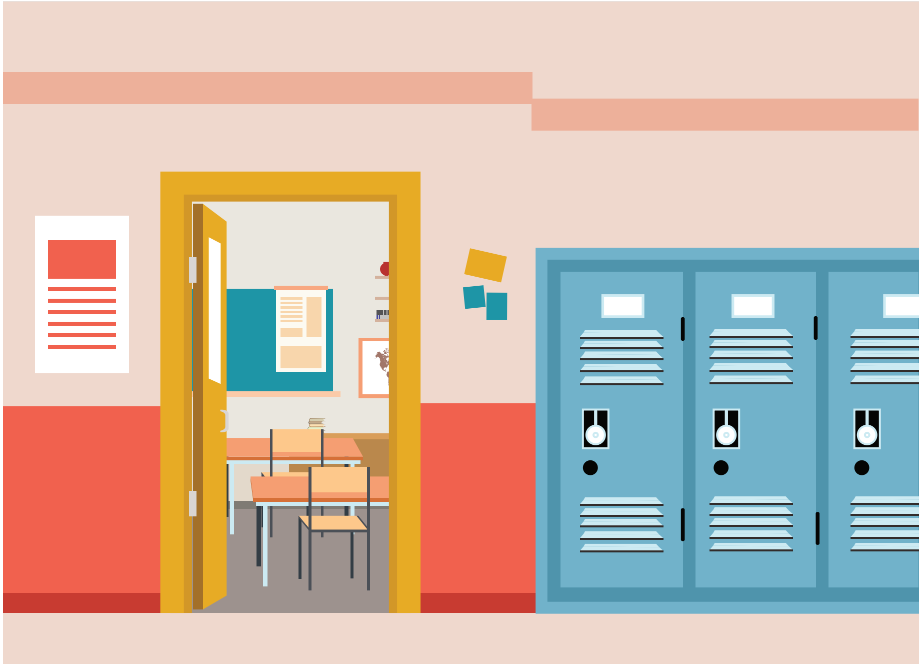
DMP
Tue 5:35 PM
Panic
Doorbell
Video
Z-Wave
Events
Schedules
ALARM

Back
Garage Door

Creating a Safe Space

An Arkansas school district adopts a storm shelter solution to address tornado and active shooter threats.

By Megan Gates



I'm glad I didn't get that grant because what we have now is much better protection.

Peak tornado season in Arkansas typically stretches between May to early June, but these natural disasters can occur any time of year if the weather conditions are right.

In 2023 alone, 30 tornadoes hit the southern U.S. state—nine tornadoes touched down in March and six occurred in January and June, according to the National Weather Service. While these storms can cause major destruction and physical harm, they also disrupt the school day.

When a tornado watch is issued, school administrators, teachers, and staff know to be prepared to seek shelter once that watch turns into a tornado warning—meaning a tornado has been sighted or detected by weather radar. Some schools have a Federal Emergency Management Agency (FEMA) approved shelter to move students, teachers, and staff into when a tornado warning is issued. But at many others, students seek shelter in interior hallways, bathrooms, and other safe spaces that limit exposure to glass and potential flying debris should a tornado whip through.

This was the procedure in the Quitman School District—a rural Arkansas school district with two main buildings for kindergarten through 12th grade students—when Dennis Truxler became superintendent in July 2014. Initially, he says he worked to get a FEMA grant to build standalone safe rooms to shelter students and approximately 90 staff members at the district's facilities. But the grant never materialized, something Truxler now says he's thankful for.

"I'm glad I didn't get that grant because what we have now is much better protection," he adds. "And you don't have to relocate. There are a lot of advantages to it, and it has ballistics, so you have protection from a shooter."

Two Problems, One Solution

It started with a simple Google search in 2018. After seeing a story about a school in nearby Oklahoma installing a tornado-proof structure in a classroom, Truxler decided to search on his browser for "tornado shelters in the classroom." One of the first results to pop up was for National Safety Shelters in Florida, which sells a saferoom solution that's marketed as being tornado- and bulletproof.

Illustration by iStock, *Security Management*

As a school security administrator worried both about the potential harm natural disasters and active shooters pose to those in his care, Truxler was immediately interested. He called the Florida company and was connected with Sarah Corrado, one of the owners, who explained that their system was manufactured in Harrisonville, Missouri, just a few hours' drive from Truxler's district.

So, Truxler took a road trip to visit the manufacturing plant and meet the makers behind the technology, which uses ballistic level-three steel to shield occupants from harm from handgun, shotgun, and high-powered semi-automatic rifle rounds.

"The thing that really impressed me was the owner, Mike Vogt, how passionate he was about providing safety for anyone—especially school districts and students and staff," Truxler says. "The process they went through, and the time they took, to make sure the product they manufactured was going to be absolutely something that saved lives, whether it be a tornado or active shooter."

For instance, the shelters are made with quarter-inch military-grade steel and available with bulletproof windows. They have been impact tested at the National Wind Institute at Texas Tech University, carry the U.S. Army's Ballistic Steel Certification, and meet FEMA 320/361 and ICC 500 guidelines for storm shelters.

After visiting the plant, Truxler went back to Quitman and leaned on his construction background to assess the number of shelter units he would need to order to place shelters in every classroom, cafeteria, library, and gymnasium in the district. He sent his estimates to the National Safety Shelter team, which worked with Truxler to check his work and then sent him a quote: $989,000 for delivery and installation for the entire campus.

The district had access to about $1.4 million in a building fund, so Truxler put together a quick financial presentation for the school board and requested a special meeting with the five members to discuss purchasing the shelter solution.

"I just showed them how we could afford to make this purchase," Truxler recalls. "My hope was that they would take this information and think about it, come back to our regular board meeting, and approve it."

But the board was also extremely interested in the solution. It decided to vote in that special meeting and unanimously approved the purchase. The next day, Truxler set in motion signing the contract, putting down a downpayment, and making the initial order, which was delivered three months later.

Installation and Training

Initially, some teachers were skeptical of the solution and concerned that it would take up too much space in their classrooms. But Truxler was able to dissuade those fears by emphasizing that in a kindergarten classroom, for example, the solution would take up about 28 square feet of a 900-square-foot room. Teachers would also be able to decorate the powder-coated exteriors of the shelters using magnets.

School was in session at the time of delivery, so the installers would arrive on Friday afternoons to put the shelters in during the weekend—limiting classroom disruptions. Facilities in the district are located on the ground floor with a concrete pad that is at least four inches thick, so the shelters can be bolted directly into the floor. This prevents them from being dislodged by windspeeds up to 200 miles per hour—the speed of an EF-5 tornado.

Installations started with the kindergarten classrooms, moving their way up by grade across the facility. The entire process took approximately six months.

The shelter solution is virtually maintenance free, Truxler says. The only repair they have made since installation is replacing some of the handles that are used to open the shelters' doors.

"I've had to replace some of those from the movement of furniture during the summer to get the floors waxed," Truxler says. "The lowest ones, some of them have been bent. Mike sent me a whole box of replacements."

Now when a tornado warning is issued, administrators will make an announcement over the school's intercom system to move into the shelters—a process that typically takes 32 seconds to complete—to wait until the storm passes. The previous process of sheltering students in interior hallways typically took several minutes.

In the event of an active shooter, the district follows a similar process except teachers and staff are instructed to use a locking mechanism inside the shelter that prevents someone outside the shelter from opening it.

The district practices these techniques in tornado drills, but Truxler says they do not announce that they are conducting active shooter drills since "a lot of kids, students, are traumatized by active shooter drills because it makes them worry about it." Instead, the district just focuses on practicing getting into the shelters in response to a weather emergency since both responses use the same process. Teachers are simply told to use the lock mechanism when sheltering for an active shooter threat.

After installing the solution, Truxler says the feedback from students, parents, and teachers has been overwhelmingly positive. He also attributes the solution to creating a safe school culture that attracts talented teachers and students to the district.

"When we installed these, we had around 640 students," Truxler says. "…since the word has gotten out, we ended this year around 866…we're fixing to be over 900. And a lot of that is because we've had excellent teachers who apply to come work here and bring their children. We've had families that have moved here, and filed for legal choice, and a lot of those who have come, come here for the safety."■

For more information on National Safety Shelters, visit *nationalsafetyshelters.com* or call 1-866-372-1530.

Photo courtesy of Quitman School District

Insider Interference

New guidance from U.S. federal agencies seeks to help state and local officials counter the threat that malicious insiders could pose to election infrastructure.

By Megan Gates

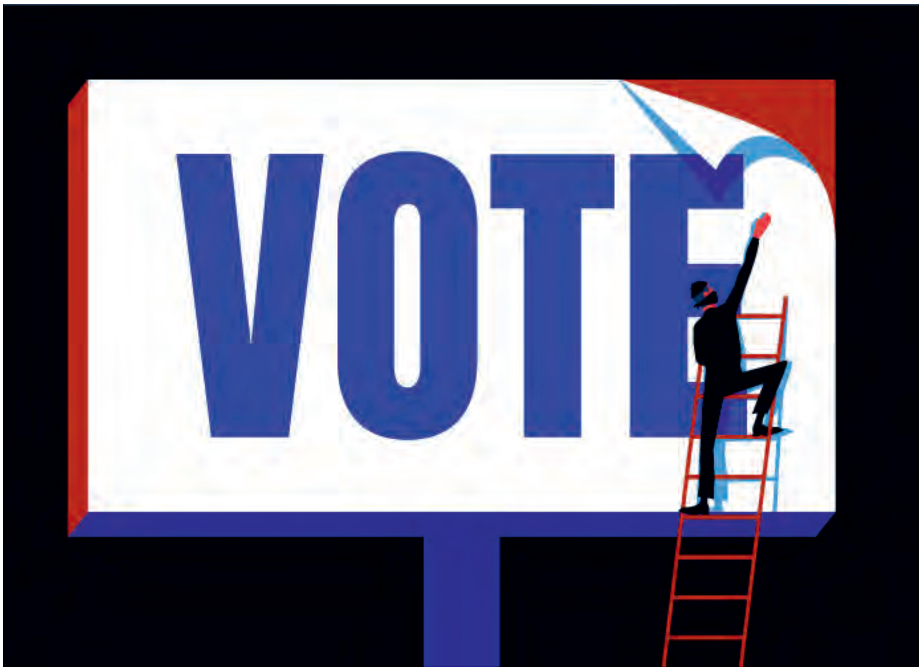


Illustration by iStock, *Security Management*

During the 2024 primary season in the United States, someone was granted access to a government office where they plugged in an unauthorized laptop to connect to a government election network.

The individual accessed data from the network, which was later shared at a public gathering where perceived election fraud issues were being discussed. A county official reported the attempt to gain access to the network, but it is unclear what ramifications the individual responsible for the breach faced.

The incident is just one of four recent examples of election infrastructure-related insider threats that the FBI, the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the U.S. Department of Justice (DOJ), and the Election Assistance Commission shared in guidance published earlier this year about addressing insider threats in the 2024 election cycle.

The agencies have historically worked together to safeguard election infrastructure from cyber, physical, and insider threats. They found no evidence that malicious actors changed, altered, or deleted votes—or impacted the outcome of past elections. But this year could be different if security practitioners are caught off guard.

"Over the past several years, the election infrastructure community has experienced multiple instances of election system access control compromises conducted by insider threats," according to guidance from the agencies. "While there is no evidence that malicious actors impacted election outcomes, it is important that election stakeholders at all levels are aware of the risks posed by insider threats and the steps that they can take to identify and mitigate these threats."

An insider could provide an adversary with material to develop or amplify messaging challenging election system security, results, or operations.

Threats to Watch

In the United States, state and local officials are responsible for administering elections—including ones for federal offices. This means that a wide range of people, from election workers to vendors to contractors to volunteers, carry out responsibilities for elections and pose a unique insider threat risk.

These individuals could be acting of their own volition, but they could also be motivated by foreign adversaries to compromise the electoral process.

U.S. intelligence agencies have tracked a growing number of foreign adversaries interested in monitoring election networks and attempting to influence or interfere with U.S. elections. In the 2024 *Annual Threat Assessment of the U.S. Intelligence Community,* the U.S. Office of the Director of National Intelligence (ODNI) said the People's Republic of China (PRC) might attempt to influence U.S. elections because of a desire to sideline critics of China and to magnify societal divisions.

"PRC actors have increased their capabilities to conduct covert influence operations and disseminate information," the ODNI wrote. "Even if Beijing sets limits on these activities, individuals not under its direct supervision may attempt election influence activities they perceive are in line with Beijing's goals."

ODNI is also watching malicious actors connected with Russia, since the country is anticipated to attempt to affect the 2024 election outcome to support its interests—such as limiting support to Ukraine.

Russia is the "most active foreign threat to our elections," said Director of National Intelligence Avril Haines in testimony before Congress in May 2024. "The Russian government's goals in such influence operations tend to include eroding trust in U.S. democratic institutions, exacerbating sociopolitical divisions in the United States, and degrading Western support to Iran."

Another actor on this front is Iran, especially since in 2022 Iranian cyber actors obtained—or attempted to obtain—U.S. voter information, sent threatening emails to voters, and disseminated information about elections. The ODNI anticipates that these actors have evolved their techniques to combine cyber and influence operations in campaigns that could be deployed during the 2024 election cycle.

In testimony and a statement published in July 2024, Haines said that Iran is becoming "increasingly aggressive in their foreign influence efforts, seeking to stoke discord and undermine confidence in our democratic institutions, as we have seen them do in the past, including in prior election cycles."

The ODNI has also observed Iranian government actors attempting to take advantage of protests of the war in Gaza, posing as activists online to encourage protests, and, in some cases, provide financial support to protestors.

Americans "who are being targeted by this Iranian campaign may not be aware that they are interacting with or receiving support from a foreign government," Haines said. "We urge all Americans to remain vigilant as they engage online with accounts and actors they do not personally know."

In their guidance, the agencies assessed the threat of a foreign adversary getting access to election infrastructure through an insider as minimal, but a "perceived normalization of election influence or interference" in 2024 could push adversaries to take more significant action leveraging insiders, the guidance said.

For instance, a foreign adversary might gain insider access by "exploiting a targeted insider's ideological views, providing financial incentives, or using proxy organizations or diplomatic presence to establish contact with an individual already in a position of trust or would be willing to seek out and acquire a position on behalf of the foreign actor," according to the guidance.

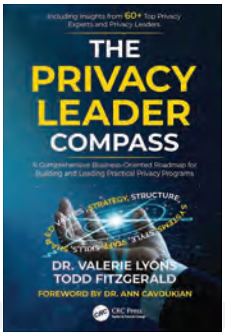
Adversaries might also consider blackmailing or coercing insiders to leverage their access, such as conducting surveillance on a person with access to gather data on financial debts, illegal activity, or embarrassing habits.

Book Review

The Privacy Leader Compass

By Valerie Lyons and Todd Fitzgerald. CRC Press; www.routledge.com/go/crc-press; 476 pages; $59.95.

In *The Privacy Leader Compass: A Comprehensive Business-Oriented Roadmap for Building and Leading Practical Privacy Programs,* authors Dr. Valerie Lyons and Todd Fitzgerald gathered the wisdom of more than 60 experts in the field and produced a helpful guide.


Including Insights from 60+ Top Privacy Experts and Privacy Leaders
THE
PRIVACY
LEADER
COMPASS
A Comprehensive Business-Oriented Roadmap for Building and Leading Practical Privacy Programs
STRATEGY, STRUCTURE
DR. VALERIE LYONS
TODD FITZGERALD
FOREWORD BY DR. ANN CAVOUKIAN
CRC Press

With that, there is a lot of data to protect. Compounded with the relatively low cost of hardware (especially when using the cloud), the importance of data risk management has never been more essential. It has also never been costlier.

European Union regulators recently hit TikTok with a $368 million fine for failing to protect children's privacy, and Meta was fined a record-breaking $1.3 billion by the same regulators for violating EU privacy laws by transferring the personal data of Facebook users to servers in the United States.

Anyone who has used Waze or other navigation tools will see they are offered a preferred route and two to three alternate routes. This is similar to privacy; this book shows there is no single way to protect data effectively and details the many ways that firms can do that.

The Privacy Leader Compass provides the reader with a broad and deep understanding of topics. From privacy law, strategies, technical implementations, people, and much more, the reader comes out with an in-depth knowledge of the many aspects of this monstrosity called privacy. The 60-plus chapters in the book quickly get to the point and give the reader actionable information he or she can use.

Many of the experts include penetrating questions that a data protection officer (DPO) or chief privacy officer (CPO) will have to ask themselves. Their boards will be looking for answers that will reassure them that corporate data is indeed being protected adequately.

For those looking for a solid introduction to data privacy and wanting to glean the wisdom of the very smart privacy crowds, *The Privacy Leader Compass* is an important book to have in their library. With privacy regulators out in force, it might also be one of your best investments.

Reviewer: Ben Rothke, CISSP, CISM, CISA, is a New York City-based senior information security manager with Tapad.

Once an insider is willing to act, adversaries could use the individual to get access to election systems to expose voters' personal information, limit voters' ability to access accurate information on Election Day, or make election systems inaccessible to the public or election workers.

"In addition, adversaries could also employ insiders to assist with their malign influence operations to undermine American confidence in the security and integrity of the elections process," the guidance explained. "An insider could provide an adversary with material to develop or amplify messaging challenging election system security, results, or operations."

Indicators of Compromise

Insider threats often exhibit red flags that security practitioners should be aware of so they can respond proactively.

When it comes to elections, the agencies provided a list of unique warning signs that practitioners should watch for. These include attempts to alter or destroy ballots or documentation without prior approval; accessing systems, equipment, or facilities without need or authorization; turning off security systems; disregarding two-person rule requirements; taking proprietary material home in any form or copying proprietary material without need or authorization; remotely access computer networks at strange times; disregarding computer policies on installing personal software or hardware; and intimidating or threatening other staff.

The agencies also recommended that election administrators and partners work together to create an insider threat mitigation program to identify gaps in current practices and create a more informed approach to risk management.

"Organizational culture should also reinforce proactive reporting of employee concerns and security issues as a core component of securing the environment," the guidance explained. "From this foundation, a successful insider threat mitigation program should implement practices, strategies, and systems that limit and track access across organizational functions ...Preventative measures against insider threats also contribute to detecting threats by establishing transparent, auditable election systems and processes, and then identifying outliers or anomalies for investigation."

For election security practitioners, the agencies said insider threat mitigation programs should include standard operating procedures for completing tasks, such as requiring a two-person minimum for sensitive tasks.

The agencies also suggested implementing physical and digital access control systems to detect and prevent insider threats, with access privileges changing leading up to Election Day or other key dates to reduce the potential for harm to physical or digital systems. This should include access logs and control forms to assist with post-incident investigations or serve as evidence.

One challenge around access control for election workers is access to the voter registrations database system, according to the guidance. "It is important for jurisdictions and state offices to work together to regularly confirm and update a list of authorized users and associated privileges," it said.

Election insider threat programs should have chain of custody procedures to track physical and digital assets, documenting each time the asset was handled and who was responsible for that interaction. Programs should also implement Zero Trust security, verifying every request for access and potentially creating a two-person rule or bipartisan teams when accessing sensitive resources.

Finally, all incidents of insider threat activity should be reported to the appropriate authorities to be investigated or documented to reduce the likelihood of similar activity in the future.

"Altogether, these measures support the integrity, reliability, and security of an election, providing the evidence to build public confidence in the process," the guidance explained. ■

CEIA USA • WEAPONS DETECTION THROUGH ELECTROMAGNETICS

GAME DAY AT RECORD SPEED.

OPENGATE® *Groundbreaking Weapons Detection System*

- Quickly and automatically screen guests with their backpacks 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

U.S. DEPARTMENT OF HOMELAND SECURITY
DESIGNATED
SAFETY ACT
www.safetyact.gov
SCIENCE AND TECHNOLOGY ®

Our Weapons Detection and screening systems take the guesswork out of security screening. Incorporating the latest in threat detection technology, CEIA (CHAY-ah) 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**.

CEIA® USA
WWW.CEIA-USA.COM

CEIA USA, Ltd. All rights reserved. CEIA USA reserves the right to make changes, at any moment and without notice, to the models (including programming), their accessories and options, to the prices and conditions of sale.

See us at GSX Booth 1620

The Art of Concierge Guarding

When debating security policies, procedures, and technologies in a fraught world, don't dismiss the unique value of positive human connection.

By Sara Mosqueda

Illustration by Taylor Callery

SECURITY
OFFICER

A guard's presence can convey a sense of security—the uniformed private officer taking note of people as they approach valuable items to prevent theft or patrolling the grounds to deter a physical breach.

However, an increasing number of security leaders are also using guards to support customer or visitor services, not dissimilar to a hotel's concierge, with the goal of improving the overall experience for residents, visitors, or clients.

The World Security Report 2023, published by Allied Universal, found that approximately 90 percent of security leaders increasingly place value on people skills instead of physical attributes like strength.

"More than nine in 10 CSOs agree that the following skills are highly desirable: emotional intelligence at 95 percent, a higher education degree at 96 percent, and the ability to speak multiple languages at 94 percent," according to the report.

The survey of 1,775 CSOs in 30 countries found that 67 percent of respondents rated customer service skills as extremely important among frontline security officers. In comparison, only 49 percent of respondents said that a background in military or law enforcement was extremely important.

Ben Olalde, vice president of retail locations for Allied Universal, notes a significant shift in what retail clients hope to accomplish with guards—moving away from having guards directly confront, accuse, and attempt to apprehend visitors suspected of stealing from a store.

"It's a lot different than it was back in the day because so many retailers aren't even allowed to make a stop," Olalde says.

It's difficult to balance the need for a welcoming atmosphere with the preservation of valuable cultural assets.

Retailers now want security officers to interact customers and visitors with ill will with the approach of "customer service them to death," Olalde says. The goal is to avoid violence altogether by having a strong security presence with a customer service focus, which will ideally deter theft and future attempts to steal from a store, stop a confrontation from turning violent, or even curb potential litigation.

In Portland, Oregon, local angler Nguyen Cao is suing a bait and tackle store and the guard company it hired. Cao claims the store's manager and a security guard falsely accused Cao of shoplifting before forcibly removing him from the store, assaulting, and threatening him. Cao said he was racially discriminated against when the store's manager confronted him in January 2023, accusing Cao—a regular customer of the store—of shoplifting, according to the lawsuit.

Although Cao offered to be searched and asked to stay until police arrived to investigate, the manager instead chose to remove Cao from the store. The store's guard, upon orders to remove Cao, threatened to arrest him, "pushed him through the front doors, threw him to the ground, and then pointed a weapon" at Cao as he got into his car to leave, court documents said. Cao, who is also accusing the companies of negligence in use of force, is seeking up to $250,000 in damages in the suit against the store, which is a local chain, and the security services company. (*Nguyen Cao v. Fisherman's Marine Supply, Inc., Talon Protection Group LLC, et al.*, Circuit Court of Oregon for Multnomah County, No. 23-cv-20230, 2023)

An officer stopping someone and accusing him or her of theft could leave a retailer open to a lawsuit if the officer was incorrect. "It's a very litigious world," Olalde says.

Welcome to the Museum

While concierge security is a growing interest in several sectors, some museums have already found a balance between offering visitors a welcoming and approachable atmosphere with the stoic responsibilities of safeguarding a building, its cultural assets, staff, and the people who come to admire the artifacts.

"You're there to help guide the experience, from the screening process to wayfinding around the museum," says Robert Carotenuto, CPP, PCI, PSP, senior manager for public safety at the Brooklyn Museum with roughly 30 years of experience in museum security. "And some officers are very knowledgeable about the institution that they work for and very well educated about the arts, so they can sometimes educate some of the visitors."

Some museums, including the Guggenheim in New York City and the Baltimore Museum of Arts have highlighted their security officers' knowledge about art on social media and in guard-curated exhibits.

While a traditional security approach still applies—with a focus on protecting the artwork and artifacts—museum guards' other responsibilities overlap with visitor services to improve visitors' experience and encourage them to return.

"It's difficult to balance the need for a welcoming atmosphere with the preservation of valuable cultural assets," notes Doug Beaver, CPP, corporate director of security for the National Museum of Women in the Arts (NMWA) in Washington, D.C. "It's essential to create a memorable and educational visit for our visitors to NMWA."

A visitor services approach is one that can help both visitors and guards as soon as someone walks into a museum, according to Carotenuto. Initial screenings at museums have become more involved in recent years, but advances in technology can cut down on wait times or allow for a hands-off approach. A guard's attitude in being welcoming instead of appearing suspicious can also support a guest's overall experience, letting the patron feel welcomed instead of scrutinized.

This can be conveyed through tone of voice and body language as much as what is verbally said to visitors.

"You want to treat people the way you would want to be treated," Carotenuto says. "If you go out someplace, do you want people to be yelling at you and nasty to you? No."

This welcoming environment can also help guards, encouraging positive interactions between visitors and staff instead of fostering a sense of surveillance or hostility. Those positive interactions are more likely to result in a safer workplace for the museum's employees, according to Carotenuto, and can decrease the chances of an altercation where staff are targeted. Ultimately, these welcoming interactions can also support the museum's overall brand reputation, conveying an open and friendly culture to visitors and encouraging them to return.

"Every institution has a brand. It's how you look and how you want to be perceived, so your physical composure needs to match all of that, too," Carotenuto says.

The focus on interpersonal skills in concierge security doesn't rule out the use of technology, though. Recent research from ASIS International and the Security Industry Association (SIA) that surveyed more than 1,700 CSOs in 30 countries found that security officers are now required to leverage technology to "augment and enhance the guarding operation," according to *Complexities in the Global Security Market: 2024 through 2026*.

The guarding market is using technology to "ensure that guards are more efficient and, operationally, spend time on higher-value activities," the report said.

For instance, the NMWA underwent a top-to-bottom renovation in 2021. Before the museum reopened in October 2023, Beaver invested in a communications system for his team of 35 security personnel. The system features a translation function, able to identify and translate between 21 different languages.

"It bridges that communication gap that we've had with international visitors in the past," Beaver says. "…This is really a very good piece of technology that not only allows our security team and visitor management team to communicate amongst each other, but it allows us to communicate with our international visitors as well."

When a visitor approaches a guard with a question but is unable to effectively communicate it in English, the guard can press a combination of buttons on the communication device, triggering both the device's language identification function and its function to translate the question or phrase to English. The device can also translate the guard's response in English to the other language, allowing the two parties to communicate successfully.

Training for Balance

When training security staff for NMWA, Beaver says he incorporates elements of visitor management and promotes learning about the artwork in the galleries, sometimes inviting the artists to share stories about the pieces with the guard force.

"Our security team would have a lot of information, fun-to-know stuff, to be able to tell visitors," Beaver says. These training sessions translated into better experiences for the visitors who submitted feedback, complimenting the security staff's knowledge of the collection.

"That's what it's all about in museums—have the best possible visitor experience that they can offer," he adds.

There are certain elements that can help balance a facility's team if the organization wants to take a more concierge approach to security, and these tenets can extend far beyond cultural property protection.

Along with covering foundational aspects of cultural security, such as how to protect different artwork, the training modules Beaver developed place an emphasis on implementing an effective visitor management program. This calls for treating every visitor with the same level of respect and giving each person "an equal opportunity to enjoy a meaningful cultural experience," Beaver says.

"We don't initiate with visitors because we understand that many visitors are coming in here to engage and interpret the artwork, and that takes some pretty deep thought processes. So, that's one of the ways that we ensure that our visitors enjoy their visit here," Beaver says.

And while guards at NMWA do not approach visitors to engage in idle conversation, they are trained to not only be ready to respond to questions from visitors, but also to be happy and excited at the interaction.

To accomplish this, Beaver emphasized interpersonal skills in the training modules, including active listening, communication, conflict resolution, and emotional intelligence.

"Conflict resolution is an important part of it, one that includes understanding the escalation cycle, situational awareness, and other strategies that can be used to calm a situation before it gets out of hand," Beaver adds.

Conflict resolution has previously been helpful in mitigating instances where someone enters the museum with the intent to harass visitors instead of to appreciate the artwork.

"Our location is such that we on occasion have undesirable situations that take place in the museum that require soft skills and de-escalation skills, and that's why this training is so important," Beaver says. Every museum employee is required to undergo conflict resolution training.

This training came into play in February 2024 when someone experiencing a mental health crisis assaulted two people from New York who were visiting the NMWA, according to Beaver. The museum's visitor service team assessed the situation and asked the perpetrator to leave.

"The individual refused to leave when asked, and at that point a visitor services team member engaged the individual in a calming conversation—one of the strategies taught in conflict resolution training," Beaver says.

A member of the team called a security manager, who continued to engage in conflict resolution and de-escalation strategies until the person left the museum without causing an additional incident.

Active listening can also support de-escalation efforts, helping defuse a tense situation.

"Let that person speak instead of interrupting them—let them get it out, hear their point of view. And then you can use that because now you understand what their issue is," Carotenuto says.

Once a guard understands the issue at hand, he or she is usually better able to address the problem in a way that may satisfy all parties. In some instances, giving a person the chance to voice their frustrations and know that he or she is heard is enough to calm a situation entirely.

Beyond interpersonal skills, other elements can support organizations that want to offer concierge security.

Security guards walk through the renovated European painting wing at The Metropolitan Museum of Art during a press preview on 16 November 2023. (Photo by Bryan R. Smith, AFP, Getty)

"You want a diverse group of people, and we have to admit that security officers [work in] extremely diverse communities," Carotenuto notes.

Throughout his career, Carotenuto worked for various cultural properties in New York City, including the Metropolitan Museum of Art, The New York Botanical Garden, and The Shed.

"When you start to talk to your staff, you realize how much they know and what their life experiences are and how they can share that. …I think that that is conveyed to visitors as they walk through your door and walk through your galleries," he says.

Handling Unwelcome Behavior

While guards are historically trained in how to deal with a potentially violent attacker or someone attempting to steal an artifact from a museum, cultural properties are high-profile places, and the threat landscape now includes activists and protesters.

These protesters may try to amplify their message by defacing or threatening museums' artwork through various means—including smashing protective glass or throwing paint, spray paint, tomato soup, mashed potatoes, pumpkin soup, or glue at a famous work of art. *The Guardian* reported that there were at least 38 incidents in 2022 where environmental protesters staged a disruption in a museum in the name of climate issues.

While most of these recent incidents occurred in Europe, other regions have not been immune from these demonstrations. In late 2023, an environmental activist defaced a memorial to a Black Civil War soldier at the National Gallery of Art in Washington, D.C. The activist used red paint to vandalize the memorial, resulting in more than $700 in damage.

For security, this issue is a thorny one. Visitors can hide in their possessions paint, glue, and food that would not be flagged as a weapon, even during screening processes.

"There are new challenges where protesters have posted on social media that they will disregard security officer instructions, that they will look to bypass screening measures," Carotenuto adds.

This strains security guards' efforts to welcome all visitors, because their efforts to ensure a safe environment will be divided with the need to monitor for activists hoping to slip in with an item that could damage artwork.

Another challenge arises when one or more protesters are successful in staging an incident, especially if the activist refuses to comply with security officers' instructions. From the museum's perspective, these incidents can damage artwork and damage the museum's reputation. These events can also discourage people from visiting the museum in the future.

Beaver adds that he has been working with other museum security directors in the New York and Washington, D.C., areas to develop a strategy to deal with protesters and minimize a negative visitor experience.

The first step is to quickly and calmly separate visitors from the site of the demonstration, which lessens protestors' ability to use the disruption as a platform for their message, he says. In some instances, security team members instruct visitors to leave the gallery and set up a separation panel around the activists. This tends to calm down these situations, and without an audience, the protesters often are ready to leave, Beaver says.

Because these activists are generally non-aggressive and focused on relatively peaceful, if obnoxious, attempts to create a platform for a cause, there is an emphasis on maintaining peaceful interactions with museum staff. Carotenuto points out that if museums search for opportunities to connect with activists targeting their galleries, it can create an ultimately positive relationship between the two parties.

Searching social media for flags or other indicators that the museum has become a target of a planned demonstration can at least prepare a security team for the presence of protesters. But it can also be used to initiate an outreach. The museum can ask the group to avoid damaging the artwork while protesting at the museum. Giving activists space for a dialogue can also open the door for a productive relationship, potentially shifting the dynamic towards a more positive and respectful interaction between the protesters and members of the security and visitor services teams, according to Carotenuto.

"Security is all about mitigation. We don't want any objects to be damaged in any way," he adds.

How Balance Can Support the Brand

Both Beaver and Carotenuto point to how a concierge security approach can reinforce an organization's larger goals—including brand reputation, workplace safety, and repeat business.

"Museums and cultural properties are all about earned income," Carotenuto says.

Using a concierge security approach in museum settings increases the likelihood of repeat visitors. Creating a respectful and welcoming environment towards visitors is also likely to increase workplace safety.

"The side effect is that if you treat people well and they feel respected and heard, they won't be angry with you. If they're not angry with you, chances are that they're going to show respect and reverence for not only your institution, but for your staff and the works of art that you're safeguarding," Carotenuto says.

When training members of his security and visitor services team, Beaver stresses to them how influential a negative experience can be and the kind of impact it can have on a museum.

He points out how, especially in the age of social media, just one visitor's negative experience can generate a "compound effect," with one social media post able to be reshared or reposted countless times. "One complaint can mushroom out into hundreds of complaints," Beaver says.

Instead, the goal for these teams is to create "the best possible visitor experience that they can offer," Beaver adds. "It really is a balancing act, but we work very closely with visitor services to accomplish that." ■

Sara Mosqueda is associate editor for *Security Management.* You can connect with her on LinkedIn or on X, @XimenaWrites.

VISIT US AT BOOTH 1588
EXHIBITOR
GSX
GLOBAL SECURITY EXCHANGE
23-25 SEPTEMBER 2024
ORLANDO, FL, USA

RETROFIT SECURITY GLAZING

Safeguarding At-Risk Facilities Inside and Out

DefenseLite® and BulletShield offer seamless glass protection, safeguarding against forced entry, natural disasters, vandalism, and theft. Ideal for retail storefronts, schools, data centers, government buildings, and other at-risk facilities, our advanced solutions ensure peace of mind and enhanced security.

- Protect property, employees, and inventory
- Clear security shields integrate with existing structures
- Services Include:
  - DefenseLite anti-intrusion panels
  - BulletShield anti-ballistic glazing systems
  - Nationwide installations
  - Threat level assessments
  - Safety & security window films

IMPACT iS SECURITY
A LIMITED LIABILITY COMPANY

DEFENSELITE®
BULLETSHIELD™

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

See us at GSX Booth 1588

ACT

As children grow and learn, they often test new behaviors, push boundaries, and overreact to stressors. Behavioral threat assessment and management teams must take these growing pains into account when analyzing threats.

By Claire Meyer

YOUR

Photo by iStock

AGE

"I hate everything."

"I don't ever feel happy." "I'm going to hurt you." These phrases are alarming and should spark concern, no matter who utters them. But when it comes to assessing threatening behavior in children, additional nuance comes into play.

"In K-12, children are growing and developing—they are experimenting with behaviors, they are responding to things like bullying, and so some of the things that might be indicative of an elevated violence risk in adults may not necessarily be indicative of a violence risk in children," says C. Joshua Villines, CPP, PCI, PSP, executive director of the Human Intelligence Group. Villines is also heavily involved in the ongoing development of a new ASIS standard on school security.

"Sometimes kids are just being kids, sometimes kids are being dumb, sometimes kids are behaving inappropriately but in a way that is age-appropriate," he continues. "You want to take the guidance from behavioral threat assessment and tailor it to the developmental stage of the population that you're working with."

Children are learning to cope with their emotions and new stressors, including social and educational pressures, so warning signs in adult behavioral threat assessment—apparent impulsivity or a low tolerance for frustration, for instance—can be very common in K-12 students.

Through behavioral threat assessment, school teams can seek to answer: If a student made a threat, does that student pose a threat?

Security professionals and behavioral threat assessment teams need to evaluate comorbidities that would layer up with impulsive or disruptive actions to increase the likelihood that a child will lash out or cause harm, Villines says. Those comorbidities could include an ongoing pattern of disruptive or dysregulated behavior, access to weapons (particularly in a region where firearm access is uncommon or heavily restricted, such as in urban areas), sudden changes in self-care (such as cleanliness or nutrition), or behaviors indicative of psychosis.

"Behavioral threat assessment is intended to be preventative," Villines says. "It does integrate very well with traditional crime prevention measures because once you've identified those behaviors of concern, when it comes to managing them, many of the management strategies that we employ to adjust the security posture of the location are traditional physical security measures." Those measures can include deploying personnel or changing up access control, but effective threat assessment and intervention also involves management strategies outside traditional security, including bringing in mental health, conflict resolution, or anger management resources, which is where non-security professionals are invaluable.

Behavioral threat assessment typically includes people from three main pillars: administration, law enforcement or security, and mental health, says Amy Lowder, director of student safety and wellbeing at Cabarrus County Schools in North Carolina.

Each individual brings different attributes to the table: the administrator represents the school and is more likely to have a relationship with the student in question; school resource officers (SROs) or law enforcement personnel can highlight legal, compliance, and social services needs; and mental health professionals can focus on prevention and student support, she explains.

"All of those different lenses come together, and that's how we can have a collaborative, comprehensive threat assessment process where we are really looking at those different facets," Lowder says. For example, an administrator might note that a student has had outbursts in the classroom and disciplinary action recently, and a school counselor could chime in that the student's parents recently separated, building a more complete picture of the student's situation. Those pieces of information can support a threat assessment, an intervention plan to aid the student, and then a monitoring plan to ensure the intervention is working.

At least one of the people in the threat assessment team should be an educator who can attest to age and cultural norms (such as if a bizarre and vaguely threatening phrase comes from a hit TV show or TikTok influencer that has been the talk of the classroom) and a mental health professional who has a strong background in mental health and developmental markers, Villines adds.

"While there are practitioners like me who are intended to bring a level of expertise and forensic professionalism to the process, rarely do any of us work alone," Villines says.

This team approach enables schools to take a more nuanced and trauma-informed approach to threat assessment and management, says Dr. Dewey Cornell, a clinical psychologist who has been studying school violence since the 1990s. Cornell is also involved in the development of the ASIS standard on school security.

"I recall a school principal who said, 'I'll just remove any student who says, "I'm going to kill you."' Well, it turns out threats to kill are very, very common in elementary school, and they're overreactions," Cornell says.

When it comes to those threats and other traditional early warning signs in adults, school behavioral threat assessment teams need to weigh and assess them differently. "When an adult says 'I'm going to kill you,' that's quite concerning and frightening," Cornell says. "When a 6-year-old says it, in some circumstances, yes, it's frightening but for the most part not. We have to take into account the person's age and capability, their maturity… There has to be that developmental context.

"The other thing that is different is the stakes," he continues. "We're trying to educate students whether they like it or not, or want to or not, so we're often trying to work with kids who have problems, needs, challenges, and traumas. That always has to be a factor."

The biggest source of school violence is fistfights, Cornell says. In a workplace, this is clearly unacceptable behavior, and the employer can take actions to terminate or punish the individuals involved. In a school, however, there must be some degree of tolerance, he says—if every kindergartener who hit or shoved a classmate were expelled, classrooms would soon be empty. Instead, threat assessment teams can emphasize conflict resolution, as well as discipline in a productive way.

Trauma-informed and restorative practices around threat assessment look different for each individual student, but generally they are designed to help the child manage their emotions and stressors, gain coping mechanisms, and return to the learning environment.

Some of the things that might be indicative of an elevated violence risk in adults may not necessarily be indicative of a violence risk in children.

"Trauma and stress generally can play a huge role in threatening behavior," Cornell says. "Every kid who makes a threat, think of them as saying 'I've got a problem I don't know how to solve. Something has happened, and I don't know how to deal with it.' The last resort is to make a threat of violence."

Students' behavior can also be misunderstood as threatening. Villines recalls a neurodivergent student whose behavior seemed antisocial and concerning. Educators and school psychologists took steps to work with that student on prosocial strategies, teaching the child how to interact more positively with others. This improved the whole educational environment while enabling that child to grow and learn new skills, Villines says.

Social skills are also rapidly changing in K-12 students because of stress, upheaval,

and remote learning during the COVID-19 pandemic, Lowder says. This means that some student behavior or emotional reactions to situations can seem extremely out of place to adults, who grew up in a very different school environment.

During the COVID-19 pandemic, "lots of isolation led to people not even understanding conflict resolution," Lowder says. "That's something that students typically struggled with. It's a developmental thing you go through—understanding how to deal with differences and division. But when the pandemic was happening, there was also a lot of disunity across the nation and the segregation of different types of groups or beliefs, whether political, racial, or gender. All those things just festered. Then once students got back together again, it was almost like people didn't know how to handle the commotion. It's taken a bit of time for schools to get readjusted."

In addition, the pandemic pushed more people to focus on their digital lives for interaction when in-personal socialization was off the table. As a result, more children are using social media, but they are using it inappropriately because most children are ill-equipped to actually manage the pressures of socializing online, she adds.

"We are finding that the majority of cases that come through, there is some type of social media element," Lowder says. "There is oftentimes a threat made, cyberbullying is on the rise, and that's definitely prevalent in social media."

But social media activity should be taken in context rather than as a standalone trigger for intervention, Cornell cautions.

"The vast majority of times, kids are showing off, getting attention, maybe they're in an argument with somebody and they say something provocative," he says. "This is just a red flag that you then have to pursue with interviews, with visits. We need skills in digital threat assessment—you have to be reasonably familiar with the social media that kids in your school are using and have some skill at searching it, making records of things that are concerning, and then you pursue and investigate."

Having a process in place for behavioral threat assessment and management enables schools to resist knee-jerk reactions related to a fear of school shootings, Cornell says. In 80 percent of cases, threatening behavior can be quickly resolved, and most of the remaining 20 percent relate to fistfights or minor altercations, he says. Just 5 percent of cases might involve a substantive threat that requires a more in-depth analysis, determining if the child has other stressors, home challenges, or developmental roadblocks that could heighten the risk posed to themselves or others. Having a process in place to investigate reports, evaluate threats, and provide resources as needed can calm fears and make threat assessments more fair, effective, and manageable for staff.

Every kid who makes a threat, think of them as saying 'I've got a problem I don't know how to solve.'

Although some interventions will need to be physical security ones—metal detectors, restricting student bag sizes in hallways or classrooms—Cornell notes that school officials will need to strike a balance between hardware and "heart-ware."

"We want school security people and school resource officers to be relationship-builders," Cornell says. "Law enforcement knows this in terms of community-oriented policing. You want to be part of the community, linked to the community, and then the community will come forward and share information with you. That's really what threat assessment hinges on. You cannot do threat assessment if you don't have people willing to share information, to report what they've seen or heard. You can't do that if you don't have a climate where people feel comfortable."

Successful security professionals in this area will have empathy, good communication skills, and an interest in being able to interact and talk with kids. This establishes the security officer as a trusted adult that students can confide in about potential threats or problems.

"It doesn't have to be that fancy," Cornell says. He recalls a school resource officer in Tennessee who started a fishing club for kids who didn't have another club where they could fit in. "It was a very relaxed, laid-back, low-stress activity," he says, noting that not everyone wants to play sports or perform on stage, but everyone can learn to fish. "He gathered a lot of kids who just wanted to be part of a group and be accepted… It's not rocket science, but I was just very taken that he had this novel idea and it worked."

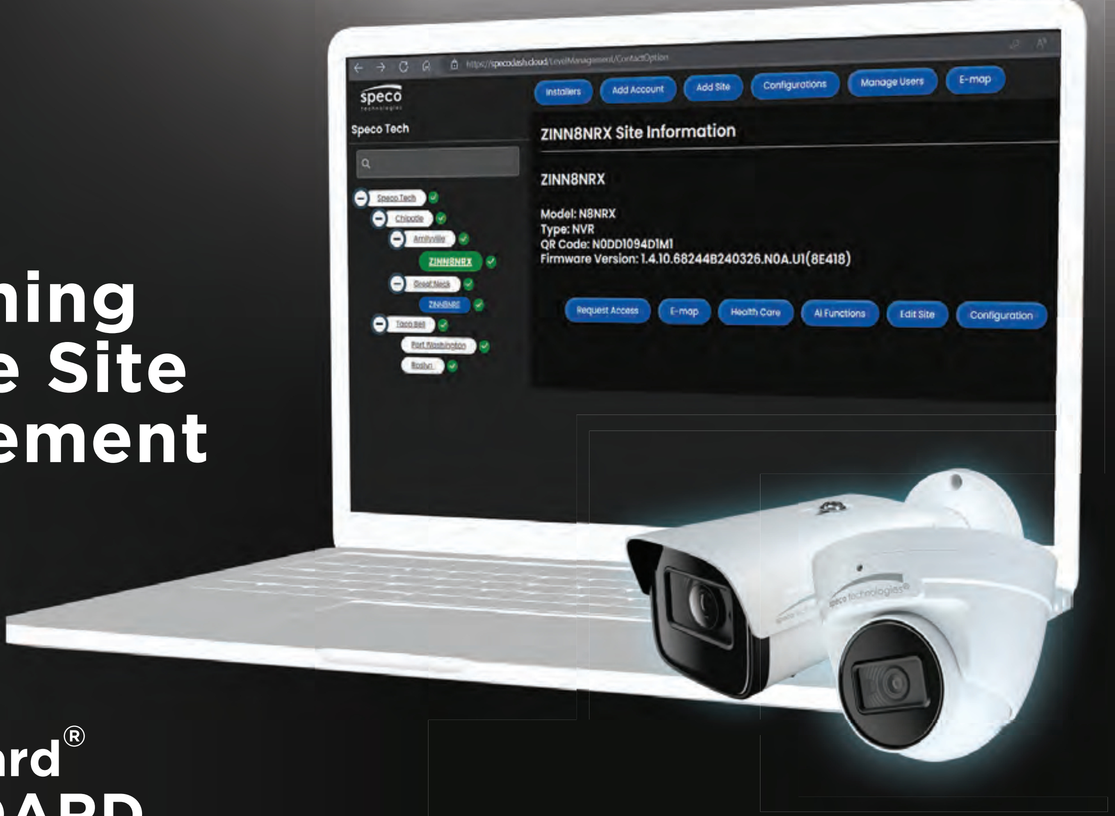
In North Carolina schools, Lowder started hosting awareness talks for the community, including students and parents, about behavioral issues, trending activities, and mental health support. These talks encourage more connection across the community and help build up partnerships between law enforcement, school officials, parents, and mental health professionals. Cabarrus County Schools also implemented weekly discussion topics across the school district so that all grade levels can focus on the same social-emotional subject but in developmentally appropriate ways. For instance, Lowder says, one week focused on perseverance and how to build up that skill. Broadly, these sessions are intended to boost students' personal resilience.

"Resilience is a huge protective factor that is oftentimes overlooked in schools," she says. "It's being able to help students understand emotional regulation… We train students on how to get their brain back in line and get their emotions regulated. It's an immediate reset that teachers have been able to do in the classroom. Even taking a sip of water can be a simple solution. We're trying to help students know that they've got a toolbox of different things that they can do to build that resilience, reconnect to their emotions, and start to make logical decisions about how they're feeling." ■

Claire Meyer is editor-in-chief of *Security Management.* Connect with her on LinkedIn or contact her directly at *claire.meyer@asisonline.org.*

speco technologies

Redefining Remote Site Management



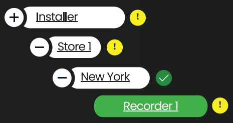
ZINN8NRX Site Information

ZINN8NRX

Model: N8NRX
Type: NVR
QR Code: N0DD1094D1M1
Firmware Version: 1.4.10.68244B240326.N0A.U1(8E418)

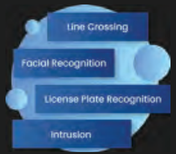
SecureGuard® DASHBOARD

THE CLOUD BASED REMOTE MANAGEMENT PLATFORM



Prevent System Down Time

Enables real-time site management and communication.



Configuration

Configure hardware and analytics remotely.

Recurring Monthly Revenue

Remotely manage and maintain locations without onsite visits.

Remote Passwords

Change the password of a user for a single site, or multiple site deployment with ease.

Request Connect

Request Connect*

Dashboard managers can secure video recorders, letting site owners control access and receive notifications when live or recorded video access is requested.
*Available upon request.

QR Code Connections

QR Code-based network connections via Mobile App for field Installations.

Manage Users Access

Assign account access and dashboard tasks by creating users

Healthcare

Remotely view system health for all SecureGuard® Dashboard installs.

EMaps

Insert floorplans to identify cameras needing attention.

Interested in learning more?

Scan to visit the SecureGuard® Dashboard Page

Follow us at Speco Technologies

Contact us 1.800.645.5516 or visit specotech.com

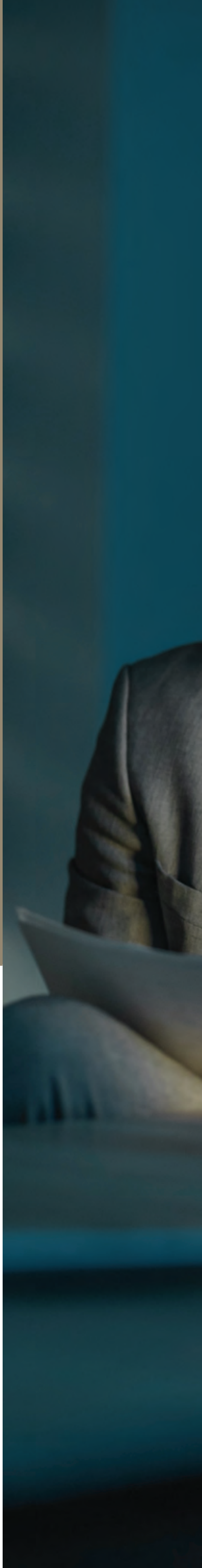
BLACKCLOAK™

blackcloak.io

Enterprise security is your job.

Personal cybersecurity is ours.

Protect executives from personal cyber threats that can compromise your business.



Digital Executive Protection.

Grappling *with* AI Guardrails

The European Union enacted the world's first comprehensive regulation of artificial intelligence, creating a new business and operational landscape for security practitioners in member states.

By Megan Gates

Illustration by iStock; *Security Management*

Almost six years after the European Union (EU) set the global standard for privacy regulation, it's made similar moves with regulation of artificial intelligence (AI) systems and technologies.

The EU AI Act was originally proposed in April 2021 and was passed by the Council of the European Union on 21 May 2024. The act entered into force on 1 August 2024—20 days after its publication in the Official Journal of the EU.

Dragoș Tudorache, civil liberties committee co-rapporteur and MEP representing Romania, said in a statement that the EU has now linked the concept of AI to the fundamental values that form the basis of member states' societies.

"However, much work lies ahead that goes beyond the AI Act itself," Tudorache said. "AI will push us to rethink the social contract at the heart of our democracies, our education models, labor markets, and the way we conduct warfare. The AI Act is a starting point for a new model of governance built around technology. We must now focus on putting this law into practice."

Alongside the EU's AI Innovation Package and Coordination Plan on AI, the AI Act will help guarantee the safety and fundamental rights of people and businesses in relation to technology.

"The AI Act is the first-ever comprehensive legal framework on AI worldwide," according to the European Commission.

"The aim of the new rules is to foster trustworthy AI in Europe and beyond, by ensuring that AI systems respect fundamental rights, safety, and ethical principles, and by addressing risks of very powerful and impactful AI models."

The act covers entities in the EU but also applies to providers and deployers of AI systems outside the bloc who could be contracted to process data collected in and transferred from the EU. Lawmakers crafted the act in this way to "prevent the circumvention of this regulation," the text of the AI Act explains.

The act does carve out exemptions for arrangements with public authorities in third countries who are working to carry out tasks in support of law enforcement or judicial cooperation. The act also exempts providers or deployers of AI systems used solely for military, defense, and national security purposes.

The move positions the EU as a "trailblazer in establishing regulatory frameworks for AI," says Chad Lesch, senior vice president, strategic projects, at Crisis24.

"The legislation employs a risk-based methodology, categorizing AI systems by their potential hazards and enforcing more stringent regulations on those deemed higher-risk," he adds. "This approach seeks to harmonize technological advancement with the safeguarding of individual rights and safety, potentially influencing international norms and encouraging non-EU AI entities to adopt similar standards of self-regulation."

The Security Baseline

For security practitioners, it's especially important to understand how the EU AI Act defines terms and practices that are often part of their profession.

- **Biometric categorization system:** An AI system for the purpose of assigning people to categories based on their biometric data.
- **Biometric identification:** Automated recognition of physical, physiological, behavioral, or psychological human features to identify people by comparing biometric data of an individual to biometric data of individuals stored in a database.
- **Biometric verification:** The automated, one-to-one verification—including authentication—of the identity of people by comparing their biometric data to previously provided biometric data.
- **Emotion recognition system:** An AI system used to identify or infer emotions or intentions of people based on their biometric data.
- **Sensitive operational data:** Data related to activities of prevention, detection, investigation, or prosecution of criminal offenses, the disclosure of which could jeopardize the integrity of criminal proceedings.
- **Publicly accessible space:** Any publicly or privately owned physical place that is accessible to an undetermined number of people.
- **Remote biometric identification system:** An AI system used to identify people without their active involvement, typically at a distance, by comparing their biometric data with biometric data in a reference database.
- **Real-time remote biometric identification system:** A remote system where capture, comparison, and identification of biometric data occur without a significant delay, or a short delay, for instant identification.

Another concept that security practitioners should already be familiar with is taking a risk-based approach, which is exactly what the EU AI Act does when it comes to regulating AI. It seeks to create obligations for technology based on its potential risks to humans.

- **Minimal risk:** No obligations for AI systems posing low risks to people or their rights.
- **Limited risk:** Transparency requirements for AI systems that interact with humans and generate content.
- **High risk:** Regulation of systems that could create adverse impacts to people's safety or fundamental rights.
- **Unacceptable risk:** Banned harmful AI practices considered to be a clear threat to people's safety, livelihoods, or rights.

Most AI systems currently used in the EU fall into the minimal risk category and have no additional obligations under the EU AI Act. For limited risk AI applications, such as chatbots, the AI Act introduces transparency requirements to make humans aware they are interacting with a chatbot. Providers must also label text, audio, and video content that is generated using AI.

Mark Mullison, chief technology officer for Allied Universal, says that he finds the risk-based approach the EU is taking particularly interesting.

"I think it's a useful way to look at things and, based on where AI and various AI models or systems find themselves in that hierarchy, it attracts progressively more oversight and regulation, and even in the top instance prohibits the use," Mullison says. "It's a very interesting approach. It's very well thought out, very thorough, so we'll see how it plays out."

Key to the EU's approach is focusing on how a particular AI system is used and the potential risk it poses. Take predictions,

AI will push us to rethink the social contract at the heart of our democracies, our education models, labor markets, and the way we conduct warfare.

for instance, which security practitioners have leveraged when it comes to resource allocation or staffing decisions.

"If that predictor is telling you whether a client is going to dispute an invoice, well that's pretty low risk and doesn't really attract much oversight," Mullison explains. "If that same technique is used not to predict the late payment of an invoice, but to predict whether somebody would be a good fit for a job—well now that raises the classification in the risk hierarchy and attracts more attention. It really depends on the application."

Unacceptable Risks

AI systems that are a "clear threat to the safety, livelihoods, or rights of people will be banned, from social scoring by governments to toys using voice assistance that encourages dangerous behavior," according to the EU Commission.

Looking at the EU AI Act text through a security lens, the legislation bans certain AI applications from the EU marketplace that could be used to categorize people.

Some unacceptable AI applications—such as social scoring systems—use data outside the context it was originally gathered for, and they could lead to detrimental or unfavorable treatment of people. AI systems used for risk assessments may also fall into the unacceptable risk category if they are used to assess an individual's likelihood of committing a criminal offense. The act makes an exception, however, for using these types of systems to support a human assessment of a person involved in criminal activity.

Other prohibitions include banning AI systems that create or expand facial recognition databases by untargeted scraping of facial images from the "Internet or CCTV" footage because this practice "adds to the feeling of mass surveillance and can lead to gross violations of fundamental rights, including the right to privacy," the act explained.

Technology regulation requires a balance between encouraging innovation and protecting the public, says Fredrik Nilsson, vice president, Americas, Axis Communications.

"When it comes to video surveillance, the EU AI Act places some restrictions on

using facial recognition in public places, similar to what we have seen with some U.S. states and cities," Nilsson adds. "It is good to see that some distinctions have been made based on applications and not the technology. It's important to remember that facial recognition is used by most of us every day in applications like Face ID and for business operations, like airport security and border control."

Also on the unacceptable risk list are AI systems used to infer peoples' emotions in the workplace or in an educational institution, except when used for medical or safety reasons.

A major area for security practitioners to review is their use of biometric categorization systems. These now fall into the unacceptable risk category if they use people's biometric data to infer their race, political opinion, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation. There is an exemption for law enforcement agencies' lawfully acquired biometric datasets, including images.

Quang Trinh, PSP, business development manager, platform technologies, Axis Communications, says it's difficult to tell how the EU AI Act will affect the deployment and use of AI-based biometric identification systems.

"That said, biometric data is used in many consumer and commercial systems, so I expect that there will be increased feedback from private entities during the implementation of the law," adds Trinh, who is also co-chair of the ASIS International Emerging Technology Community Steering Committee. "This discourse is sure to encourage risk assessments and address privacy concerns in order to ensure safe and lawful use of biometric data as a component of a safety and security system."

Under the act, using AI systems for "real-time" remote biometric identification of people in publicly accessible spaces for law enforcement purposes is generally prohibited. But there are exceptions here, too. Law enforcement can use real-time identification in defined situations—such as searching for victims of crime, like reported missing people and human trafficking victims; threats to the life or physical safety of people, including terrorist attacks; and identifying perpetrators of designated criminal offenses—with authorization from a judicial authority or an independent administrative authority.

Law enforcement is also limited to deploying these systems to confirm their targets' identity, with additional limits on the time, geography, and personal scope for the system's use.

"The use of the real-time biometric identification system in publicly accessible spaces should be authorized only if the relevant law enforcement authority has completed a fundamental rights impact assessment and…registered the system in the database as set out in this regulation," according to the act.

National market surveillance authorities and national data protection authorities are then required to submit annual reports to the EU Commission about how law enforcement is using real-time biometric identification systems.

It's unclear how these provisions will affect private security activities today, but Mullison says that it might influence how people are exploring using more advanced methods of security.

AI in Action

Learn more about recent trends in artificial intelligence in the AI issue of Security Technology, available here. ▶▶

"For instance, some of the most advanced security programs try to understand individuals and behavior," he explains. "If you start to, through your video analytics, look for people who are agitated or look for people who fit certain characteristics, that likely drops the application into the higher-risk category and either prohibits it or attracts a lot of overhead and oversight, depending on the specifics of what's going on."

High Risks

The EU AI Act categorizes high-risk AI systems partly due to the sector they are used in. AI technology used in critical infrastructure, educational or vocational training, safety components of products, employment, essential private and public services, law enforcement, border control management, and administration of justice and democratic processes could be considered high risk.

These types of AI systems may only be placed into the EU market and used if they comply with mandatory requirements, including being subject to a risk management system, data governance requirements, technical documentation mandates, record-keeping for their lifetime, transparency with deployers requirements, human oversight measures, and accuracy, robustness, and cybersecurity requirements.

These requirements also impact robotics that use AI to move or complete tasks, which will now be subject to certain high-risk requirements.

"For instance, increasingly autonomous robots, whether in the context of manufacturing or personal assistance and care, should be able to safely operate and perform their functions in complex environments," the act explained.

Systems that rely on biometric data are classified as high risk because they contain sensitive personal data. If the system produces an inaccurate result, for example, it can lead to biased or discriminatory effects for an individual. But this classification is not universal.

"Biometric systems which are intended to be used solely for the purpose of enabling cybersecurity and personal data protection measures should not be considered to be high-risk systems," the act clarified.

Classifying biometric identification systems as high-risk will significantly impact their use in Europe, Lesch says.

"Companies will face stricter compliance, leading to higher costs and a need for more robust oversight," he explains. "The act limits biometric use in public spaces, pushing firms to seek alternative security methods or innovate within compliance boundaries."

Lesch adds that this might help larger entities that can absorb higher compliance costs but could sideline smaller players in the market.

"However, these regulations could also boost consumer trust by ensuring biometric technologies are used transparently and securely, aligning with privacy and ethical standards," Lesch says.

AI systems that manage or operate critical infrastructure are also considered high-risk systems because their potential failure would put people's lives and health at risk at a large scale. But the act does carve out an exemption for components used "solely for cybersecurity purposes" to not be qualified as safety components, and therefore not considered high-risk systems.

"Examples of safety components of such critical infrastructure may include systems for monitoring water pressure or fire alarm controlling systems in cloud computing centers," the act added.

Employment-related AI systems also meet the high-risk mark, particularly those systems used for recruitment, promotion, and termination processes because they could impact an individual's future career prospects, their livelihood, or workers' rights.

Additionally, AI systems that are used to classify and evaluate emergency calls—such as to establish priorities for dispatching emergency response services—meet the high-risk threshold because these systems are used in critical situations for the life and health of people and their property.

Complying with the Act

At Crisis24, which is owned by Canada-based GardaWorld, Lesch provides a streamlined look at how the company will maintain compliance with the EU AI Act when it comes into effect. This will include conducting risk assessments to determine if any of its AI systems fall under the high-risk category and developing a comprehensive strategy to align all AI-related operations with the act's requirements.

"This might include revising AI deployment strategies, maintaining our platinum level data protection, and implementing transparent AI decision-making processes," he adds.

Crisis24 will enhance its data governance protocols to comply with the act's provisions on data quality, storage, and processing to ensure AI systems are used in a lawful, transparent, and secure manner. Lesch says that the company will maintain its ethical AI framework and continue training programs to ensure employees are aware of the act's requirements and compliance procedures.

Additional efforts will include ensuring third-party vendors are compliant with the act, setting up mechanisms for ongoing monitoring of the company's AI systems' compliance, and continuing to engage with legal experts to update Crisis24's compliance measures so they evolve with the implementation of the AI Act.

While Allied Universal is a U.S. company, it does business in 90 countries around the world—including EU member states—and has more than 800,000 employees. When it acquires AI technology or builds and applies its own, compliance with the EU AI Act is now something that will have to be considered, Mullison says.

"We're not terribly concerned with that because we have tried since the beginning to be transparent, ethical, and establish a governance process that internally makes sure that we're doing the right things," he adds.

Allied has an internal governance process that involves stakeholders from its legal, HR, compliance, operations, and technology teams getting together to discuss and evaluate AI initiatives, ensuring they meet its requirements and match its ethical approach to AI.

For instance, Allied began using AU Hire Smart—an AI model that helps screen job applicants—in 2020 just as the COVID-19 pandemic began. When applying for a position, applicants can schedule a traditional in-person interview, a video interview with another person, or a video interview that is evaluated by the AI system for the best potential job fit. Roughly one-third of applicants select the AI-evaluated interview option, which is designed to help speed up the hiring process.

"What it does is it gets through the screening process and gets somebody to the front of the line," Mullison says. "We trained the model based on a set of carefully crafted questions, which we asked of several thousand of our existing high-performing security professionals."

The act limits biometric use in public spaces, pushing firms to seek alternative security methods or innovate within compliance boundaries.

Based on those answers, AU Hire Smart will classify people if they seem like a great fit or not. After the AI screening, a human takes the next steps to move the applicant through the hiring process.

Part of the company's process is to regularly review the system to ensure it's not creating an adverse impact on candidates while continuing to make good—and fair—decisions on how to classify candidates for their potential fit.

"There are really two sides to the coin of evaluating the impact of AI," Mullison says. "There's a potential negative that you have to make sure that you've got structures in place to avoid, but then in doing it you get a lot of positives like understanding consistently that decisions are being made the way you want them to be made."

Meanwhile at Axis, the company has closely been following the developments of the EU AI Act and providing feedback to authorities and lawmakers, Nilsson says.

"As a global company, Axis is of course intent on abiding by all local and global regulations, and the EU AI Act is no different," Nilsson adds. "We took a similar approach with GDPR by carefully implementing the EU regulations on a global level."

Future Ramifications

Six months after the EU AI Act enters into force, its prohibitions on unacceptable risk AI go into effect with additional enforcement dates stretching through 2030. Given the breadth of the EU AI Act and the lengthy period for implementation, it will take time to understand how it will affect the security landscape in Europe and beyond.

"It's very broad, it's very thorough, and on one hand that's a good thing," Mullison says. "But whenever you take such a big swing, when that meets the specifics of all the different use cases, the impact remains to be seen."

Ashley Casovan, managing director of the International Association of Privacy Professionals (IAPP) AI Governance Center, says the AI Act is very specific in certain areas—such as how law enforcement can use biometric systems for policing—but less detailed in others. She anticipates that more information and detail will come out in implementing acts, including the development of standards.

"Given that the EU AI Act identifies that there are different types of AI systems and context that they are being used in, having a one-size-fits-all risk assessment is going to be difficult to create a standard for," she explains.

The EU Commission has the authority to issue delegated acts on how an AI system is defined, criteria and use cases for high-risk AI, and thresholds for general purpose AI models with systemic risk. The commission can also provide guidance on implementation of the requirements for high-risk AI, transparency obligations, prohibited AI practices, and more, according to the IAPP.

One area that Lesch says he anticipates changing is how entities will use biometric identification systems. He foresees that European organizations will likely adopt alternative, less intrusive, authentication technologies. These could include mobile-based authentication, physical security tokens, cryptography-based methods, and one-time passwords.

Outside of Europe, Lesch says multinational corporations may find it more practical to adopt uniform AI policies that comply with the strictest regulations that they are subject to, which in many cases might be the EU's. He also anticipates that the act may influence global supply chains since companies producing AI components or software will need to ensure their products are compliant with the EU's regulation.

"This may come at a significant cost, or companies might choose it is no longer cost feasible to do business with regions with more stringent regulations," Lesch adds.

The EU AI Act could also influence the future of where AI research and development are focused.

"This may risk shifting global R&D progress towards countries with less stringent regulations, creating a significant disruption to the geopolitical balance of power across military, economic, and geopolitical arenas," Lesch says. "While the direct legal jurisdiction of the EU AI Act is limited to the EU, these indirect effects could lead to broader changes in how AI, especially in security and biometrics, is developed and used worldwide."

Trinh adds that the EU AI Act may create global understanding and help establish international standards for data quality, privacy, transparency, and interoperability.

"What is for sure is that the EU AI Act has put a spotlight on AI, and it will encourage guidelines and regulations beyond the EU," Trinh says.

Additionally, Trinh says that he foresees the EU AI Act having a similar influence on AI policy that the GDPR had on data privacy regulation outside of Europe.

"The world is increasingly more interconnected and technological solutions serve a global audience—so the same high, ethical standards should exist everywhere," Trinh adds. "Additionally, entities such as the National Institute of Standards and Technology, or NIST, are working with the AI community to build the technical requirements to ensure AI systems are accurate, reliable, and safe. Suffice to say that a normative effect is likely and will follow the emergence of new standards." ■

Megan Gates is editor-in-chief of Security Technology and senior editor of *Security Management.* Connect with her at *megan.gates@asisonline.org* or on LinkedIn. Follow her on Threads or X: *@mgngates.*

Toxic Workplaces | By Sarah J. Powell

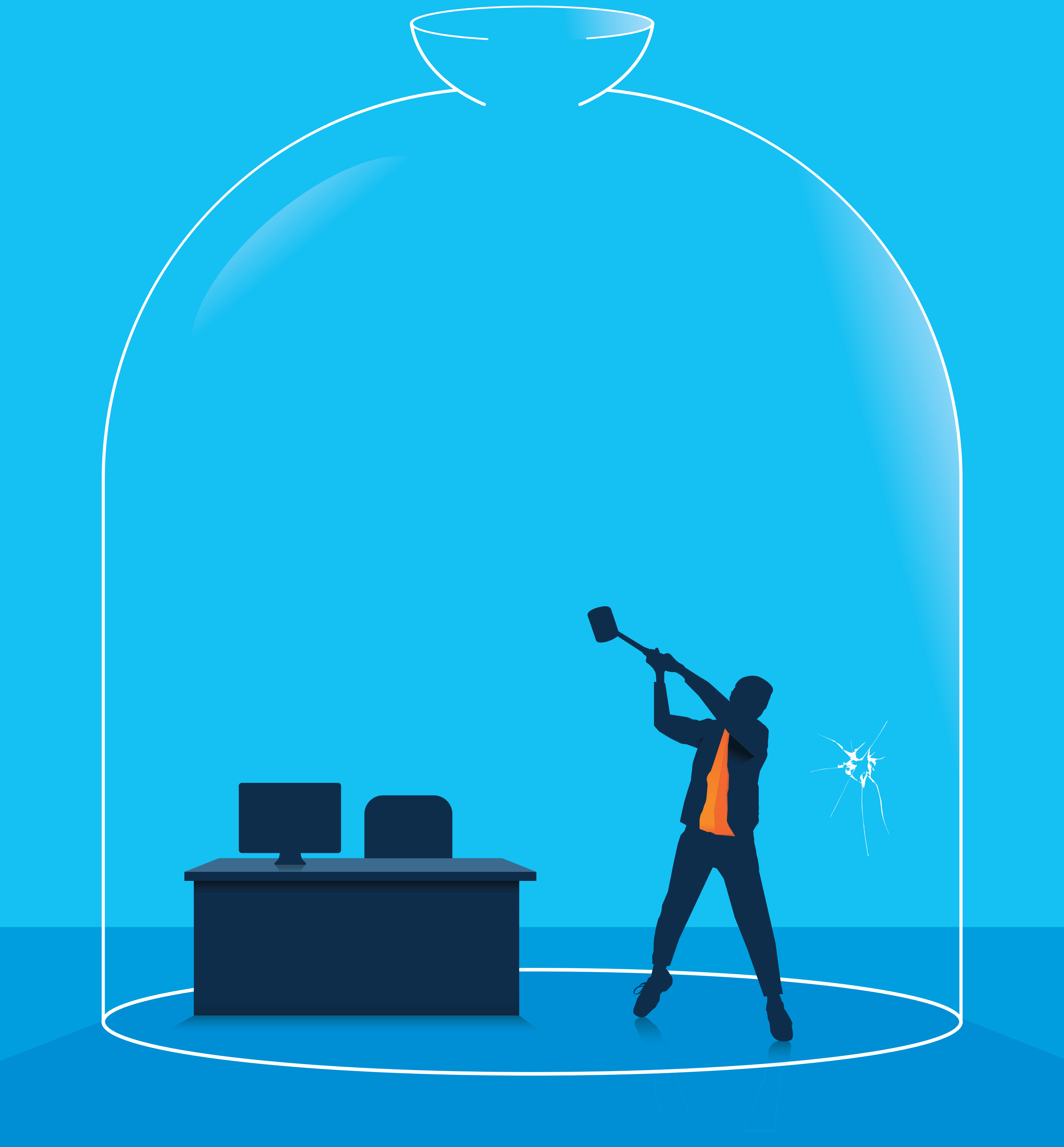


Illustration by *Security Management;* iStock

ESCAPE FROM TOXICITY

WHEN FACED WITH A TOXIC WORK CULTURE, YOUR BEST OPTION IS OFTEN TO LEAVE. BUT HOW CAN YOU MANAGE THE SITUATION IN THE SHORT TERM WHILE YOU LOOK FOR YOUR NEXT OPPORTUNITY?

BY SARAH J. POWELL

THE SECURITY INDUSTRY HAS AN ATTRITION PROBLEM.

With turnover rates that can soar to 300 percent among guard forces, the industry has severe challenges impacting operational and financial health. Drivers for security turnover include low compensation, lack of training, high risk activities, and poor work environment.

Considering that half the world boasts more security officers than public law enforcement, many people are surprised to learn that security officers often earn less than two-thirds of the mean national annual salary. Low compensation is often cited by senior leaders as the key reason for turnover, but it does not tell the whole story. In recent years, the work environment has emerged as a significant determinant in employees' decisions to stay or leave.

Across many industries, toxic workplace culture has been a leading cause for attrition. According to research published by MIT Sloan Management in 2022, toxic workplace culture was more than 10 times more likely to drive attrition than compensation. Furthermore, women are up to 41 percent more likely than men to experience toxicity at work.

IDENTIFYING THE FIVE TRAITS OF A TOXIC WORKPLACE

Defining a workplace as toxic can be challenging. Researchers describe a "toxic work culture" as an environment that negatively disrupts one's personal life due to the job, the people, or the culture. We spend most of our lives engaged in work, and a toxic workplace culture can have a massive effect on our personal well-being. Truly toxic cultures impact mental health, increase burnout, and cause declines in employee well-being. Researchers identified the following five most prominent attributes of toxic workplaces:

- **Disrespectful:** A lack of consideration, courtesy, and respect for others.
- **Noninclusive:** Ignoring diverse groups of employees and excluding them from decision-making.
- **Unethical:** Dishonesty, regulatory violations, and false promises.
- **Cutthroat:** Undermining and sabotage among employees.
- **Abusive:** Sustained hostile behavior towards employees, including bullying and verbal abuse towards subordinates.

While some isolated experiences may indicate a negative dynamic, it's important to assess whether a workplace is toxic or merely a poor fit for your needs.

ASSESSING WHETHER A WORKPLACE CULTURE IS TOXIC REQUIRES EVALUATING THE ORGANIZATIONAL CULTURE, INCLUDING VALUES, NORMS, AND BEHAVIORS.

DIAGNOSING TOXIC WORKPLACE CULTURE

Organizational culture can be disappointing and frustrating for lots of reasons, including ineffective leadership, overloaded bureaucracy, or inadequate staffing. These reasons create friction, but they don't necessarily lead to toxicity. Assessing whether a workplace culture is toxic requires evaluating the organizational culture, including values, norms, and behaviors.

Culture is made up of systems that give rise to the conditions for how organizations and teams work together. Systems, protocols, and policies are all created by humans and can lead to intended and unintended outcomes. Toxic cultures may emerge from poorly designed systems or misaligned incentives that perpetuate harmful practices and behaviors. Organizations might also have distinctions between managerial and employee cultures, which affect behavior in different ways. For example, unreasonable performance metrics tied to managerial compensation can create undue stress, leading to toxic management practices.

In a 2024 *Wall Street Journal* article, psychiatrist Dr. Samantha Boardman cautioned people to be careful about overgeneralizing other individuals as "toxic" or "not toxic." Such a reductionist binary squeezes out our capacity for empathy, understanding, and curiosity. Casually using the word "toxic" to describe someone also personalizes the problem to a single individual, rather than considering how a larger, reinforcing system may give rise to harmful behaviors. While labeling someone as toxic points a spotlight on troubling behavior, it also suggests that the person is irredeemable, with no hope for learning or growth. As Boardman writes, "We risk losing sight of their humanity."

THE EFFECT OF TOXIC WORKPLACES

Toxic work culture hinders employee satisfaction, engagement, and commitment, and it puts people in a chronic state of psychological distress. Even if we try to rationalize the situation, abusive behavior triggers an automatic stress response in our brains and pushes us into survival mode. Activation of the sympathetic nervous system gives rise to reactions such as fight, flight, freeze, or fawn. Survival behaviors like these are embedded in humans' evolutionary wiring, giving us a bias for survival. But over time, this automatic response becomes chronic, diminishing cognitive function and eventually wearing down the body's physiological systems and immune function. This wear and tear may eventually give rise to chronic disease and poor mental health.

Long-term exposure to toxic environments also has profound psychological effects, such as anxiety, depression, and even symptoms of post-traumatic stress disorder (PTSD). Relationships outside of work can also suffer, because work stress carries over into our personal lives. It's unfortunately common for people to stay too long in harmful, toxic circumstances because they believe there are few alternative options available to them or they fear a major change. But staying too long in such an environment can be detrimental.

It is important to refrain from blaming a victim of toxic culture. Such workplaces exact a heavy toll on self-worth and morale. That said, it is critical for people to realize that they do have the agency and power to make a change. Every day, we choose where we will work. While it can feel daunting at times, every employee has the choice to walk away from an employer and choose a different one. Doing so often requires a plan and a timeline, and the first step is identifying whether your experience warrants departure.

STEP ONE: DIAGNOSE THE CULTURE

All people deserve to be treated with respect, dignity, kindness, and empathy by the people for whom and with whom we work. There are no exceptions to this adage. It is becoming more commonplace to think of the employee as a "customer" for an employer, and it is up to organizations to figure out how to retain talented, loyal, and competent staff. No matter how many stories we tell ourselves, no one must stay in a work culture that is abusive and disrespectful. Use these six steps to evaluate whether your workplace experience is toxic.

Evaluate your experience. Compare your workplace to the five toxic traits outlined above. Is your workplace experience one of toxicity or mere annoyance? If systems and processes cause irritation, can they be changed? While toxicity causes harm, more common workplace friction points provide opportunities to make things better and to participate in systemic improvements.

Assess harm. Reflect on whether work interactions erode your self-worth. If toxic behavior is prevalent, consider making a change. The more your everyday work experience is influenced by toxicity, the more urgent your need to remove yourself from the environment.

Seek support. Share your experiences with a trusted confidant outside of the organization. If possible, seek out a friend or family member who is a psychologist or social worker who can offer perspective and guidance. You might also consider

WHAT SUPPORT DO WORKERS WANT FROM EMPLOYERS?

WHAT'S IMPORTANT TO WORKERS?

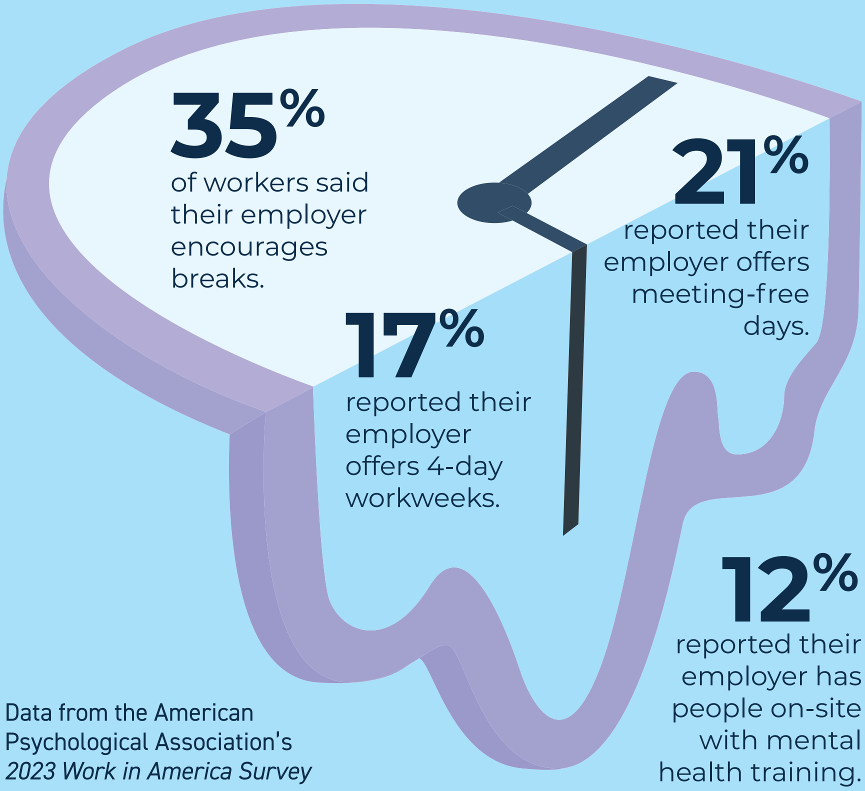
To work for an organization that values their emotional and psychological well-being.

To work for an organization that provides support for employees' mental health.

To feel respected at work.

To work for an organization that respects boundaries between work and nonwork time.

DO YOU NEED A BREAK?



35% of workers said their employer encourages breaks.

21% reported their employer offers meeting-free days.

17% reported their employer offers 4-day workweeks.

12% reported their employer has people on-site with mental health training.

Data from the American Psychological Association's *2023 Work in America Survey* seeking out a career coach who can act as a knowledgeable sounding board.

Identify self-talk. Notice if you are justifying remaining in a harmful situation and challenge these narratives. Cultural mythologies are rife with stories that we unconsciously adopt. For example, in toxic workplace dynamics, some people resort to the mythology that "The devil you know is better than the devil you don't." While this may seem a harmless idiom, it can keep people in situations that they would be much better off leaving.

Uncover biases against action. Identify negative feelings related to concepts like disloyalty, quitting, or prioritizing your own well-being. Quitting a job can inspire feelings of shame or fears of failure, but researchers like Annie Duke (author of *Quit: The Power of Knowing When to Walk Away)* have done marvelous research on why quitting can be the best action to take. As a psychologist and professional poker player, she should know. Spoiler alert: pro quitters quit fast.

Several years ago, I spoke to a woman named Lynne worked for a verbally abusive and controlling boss for many years. When the boss was finally removed from his position, I asked Lynne what she would tell her younger self if she could. She asserted, "Just leave." Lynne was struck by how many stories she had told herself that had kept her in a bad spot all those years. The simple change of supervisor opened her eyes to the fact that she'd been needlessly tolerating harmful behavior for much of her career. "I thought that I had to prove to myself that I am strong, that I can take it," she said. "But I realize now that I was simply making a choice to be put in harm's way."

INDIVIDUAL EMPLOYEES ARE OFTEN UNABLE TO CREATE SIGNIFICANT CHANGE IN ORGANIZATIONAL CULTURE UNLESS THEY THEMSELVES ARE IN A POSITION OF EXECUTIVE LEADERSHIP.

STEP TWO: CREATE A PLAN FOR CHANGE

If you've concluded that you work in a toxic environment, your next step is to plan to change roles or leave the organization. Departing for a new role can take some time, so it's important to create a plan that considers your personal circumstances. Keep in mind that individual employees are often unable to create significant change in organizational culture unless they themselves are in a position of executive leadership. While leaving a toxic workplace is often the best long-term solution, there are strategies individuals can use to manage toxic situations in the short-term.

Set boundaries. If possible, clearly define your limits regarding acceptable behavior and communicate them assertively. While this may not change poor behavior, it can help protect your well-being. Setting boundaries enables you to continue to work effectively with others. By setting up parameters for what behaviors or conditions you will and will not tolerate, you are protecting yourself first. The absence of boundaries can leave you feeling drained, disrespected, and frustrated.

For example, if you have a manager who routinely shouts at you, you can calmly and assertively respond by saying, "I do not accept being spoken to in that way. When you are ready to discuss the matter calmly, I will be open to hearing your point of view."

Seek support. Find allies within the organization who share your concerns and experiences. Support one another and find ways to collectively address toxic behaviors—if you can. Take care not to allow discussions to devolve into victimhood and helplessness. Instead, engage in productive action by sharing your concerns with peers to compare notes and emotionally support one another, respectfully seeking guidance from leaders in the organization, and collectively sharing your experiences with human resources or organizational ethics staff. Reinforce for one another the power that you all share to make a change.

Document incidents. Regardless of whether you intend to make a formal complaint to human resources, it's important to document your experience. Keep a record of toxic interactions, including dates, times, and details. This documentation is incredibly useful should you need to escalate the situation to human resources. Keep in mind that the primary purpose of the HR function is to protect the organization, and understand that filing a complaint may not result in the actions that you desire. If legal action is required at some stage, you will need to have as much tangible evidence as possible.

Practice self-care. Prioritize your health and well-being by engaging in activities that help you manage stress, such as exercise, meditation, or therapy. While self-care is not a sufficient long-term strategy for dealing with a toxic workplace, it can help you cope in the short term as you plan your exit.

Take control of your career path. Recognize your power to take control of your career path and seek healthier environments. Start letting your network know that you are looking for a new role. Ask for new introductions from those you know, and don't hesitate to reach out to people whose work or leadership you find compelling. Follow your curiosity. Consider what you value most in a workplace, such as work–life balance, opportunities for growth, or a supportive team. Reflecting on your priorities and goals can help guide your job search and help you find a better fit.

Toxic workplace culture is harmful to both individuals and organizational outcomes. Navigating such an environment is challenging, and recognizing the signs of toxicity and taking proactive steps toward change will lead to a healthier, more fulfilling career path.

By empowering yourself with knowledge and support, you can take control of your career journey and make choices that prioritize your well-being and professional growth. Remember that you always have agency to make choices about where you work. In the meantime, double down on self-care, evaluate your priorities and goals for your career, and consider a next move that will lead to a more positive, new work experience. ■

Sarah J. Powell is an applied anthropologist, change practitioner, and human-centered designer with nearly 20 years of experience in risk and resilience. As the founder of SP2 Strategies, she helps organizations cultivate resilient leaders, teams, and organizational cultures on a large scale.

Meet the New ASIS CEO

William "Bill" Tenney began as ASIS International's eighth executive on 1 July 2024. Tenney has been a security professional for more than 35 years, with experience in both the public and private sectors.

Most recently, Tenney served as chief security officer and senior vice president at MetLife. Previously, he worked in security leadership roles for Bloomberg and Target Corporation. Tenney also served in a civilian role in the national security community and as a U.S. Naval Officer for eight years.

As ASIS International's new CEO, Tenney spearheads the organization's strategic vision, working closely with members, partners, and stakeholders to advance the mission of fostering excellence in the security profession worldwide. With a commitment to collaboration and continuous improvement, he is poised to lead ASIS International into an exciting new era of growth and impact.

Success at Security LeadHER

The second annual Security LeadHER conference took place in Phoenix, Arizona, in June 2024. The one-of-a-kind conference focused on advancing, empowering, and connecting women in security. More than 400 attendees came to the day-and-a-half event, featuring electric keynotes, dedicated networking, and industry-leading presenters.

"Following the tremendous success of our inaugural event, we're thrilled to see Security LeadHER 2024 sell out with over 400 attendees from seven countries," says Mary Gamble, Esq., MBA, CPP, chair of the ASIS Women in Security Community. "This partnership between ASIS and SIA has proven to be a catalytic force to develop and promote the success of women in the security industry and will have a positive impact for years to come."

ASIS International and the Security Industry Association (SIA) are excited to continue this partnership next year with Security LeadHER 2025 on 9-10 June in Detroit, Michigan. Keep an eye on *securityleadher.org* for more information on next year's conference as it becomes available.

ASIS Celebrates the Awards of Excellence

ASIS International is proud to recognize the important work of ASIS members around the world with awards that celebrate their accomplishments and dedication to the security management profession. All award winners were honored at a ceremony on Sunday, 22 September, at GSX.

President's Award of Merit
Brian J. Allen, CPP
John A. Petruzzi, Jr., CPP
Robert Watson, CPP

Security LeadHER 2024 attendees brought their enthusiasm and experience to Phoenix, Arizona.

Security LeadHER photo by Anthologie for SIA and ASIS

Women in Security Global Community Karen Marquez Honors
Letitia Emeana, CPP, PSP, CISMP

Don Walker Memorial CSO Center Security Executive Award
Mark J. Golsby, CPP

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

Roy N. Bordes, CPP, Memorial Community Leadership Award
James T. "Tom" Roberts, CPP

NextGen of the Year Award
Shi Sheng Koh, CPP, PCI, PSP

Ralph Day Memorial Security Officer Heroism Award
Winner
Frederick Tucker, Allied Universal

Honorable Mention
Richard Gaulli, GardaWorld
Uchechukwu Nwafor, Admiral Security

Award sponsored by TEAM Software and Brownyard MacLean Specialty Insurance Services/Markel

PCB Outstanding Achievement Award
Paladin "Pj" Jordan, CPP

Distinguished Service Award
Abraham Desantiago
Alan F. Greggo, CPP
Harvindra Singh, CPP

I.B. Hale Chapter of the Year Award
Jamaica
North Texas
Phoenix

Outstanding New/ Revitalized Chapter
Doha, Qatar

Community of the Year Award
Professional Development

PCB Organizational Award of Merit
Saudi Aramco's Western Region Industrial Security Operations Department

Love GSX? Attend a Regional Conference!

ASIS International's Global Security Exchange gathers thousands of security professionals from across the world for top-notch education, networking opportunities, and an exhibit hall with the newest tech. GSX is the perfect place to keep your skills sharp and stay on top of the latest issues—but it's only once a year.

If you are looking for more events and conferences to hone your professional skills throughout the year, you're in luck. ASIS hosts and supports a variety of security events across the world and throughout the year to help you maintain your network and grow your professional knowledge.

4-5 November 2024 | Singapore

Securing Tomorrow: The Future of Security in APAC
The ASIS Asia Pacific Conference will provide opportunities for attendees to network with other leaders in the region and attend education about the most pressing security topics across the region and world. Continue to check ASIS channels for more information about the upcoming event.

18-19 November 2024 | San José, Costa Rica

Security Beyond Borders: Building the Future Together
The ASIS LATAM & CA Integrated Security Congress 2024 will bring together the most influential experts, high-level executives, and government authorities in the field of security to discuss the most pressing challenges and emerging opportunities in the industry. It will serve as an exceptional forum for establishing and reinforcing relationships, exchanging valuable knowledge, and forging strategic alliances.

4-6 March 2025 | Dublin, Ireland

From Risk to Resilience
ASIS Europe 2025 will feature inspiring keynotes from across the continent and world, 50+ educational sessions and workshops, dedicated networking time, and a security technology and solutions showcase.

More regional conferences may be announced in the coming months. Check *asisonline.org/global* for updates. ■

ASIS Global Board of Directors

PRESIDENT
Cy A. Oatridge, CPP
OSG
Tacoma, WA, USA

PRESIDENT-ELECT
Joe M. Olivarez, Jr.
Jacobs
Houston, TX, USA

SECRETARY/TREASURER
Eddie Sorrells, CPP, PCI, PSP
DSI Security Services
Dothan, AL, USA

CHIEF EXECUTIVE OFFICER
William W. Tenney
ASIS International
Alexandria, VA, USA

AT LARGE DIRECTORS
Danny Chan
Mastercard International, Inc.
Singapore

Axel Petri, CPP
Deutsche Telekom AG
Bonn, Germany

Karen Frank, CPP
KPMG
Raleigh, NC, USA

Rick Kelly, CPP
Chubb
Mechanicsburg, PA, USA

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

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

EX-OFFICIO VOTING DIRECTORS
Maria Teresa Septien, CPP
AFIMAC Global
Mexico City, DF, Mexico

Lisa Oliveri, CPP, PCI
National Democratic Institute
Aldie, VA, USA

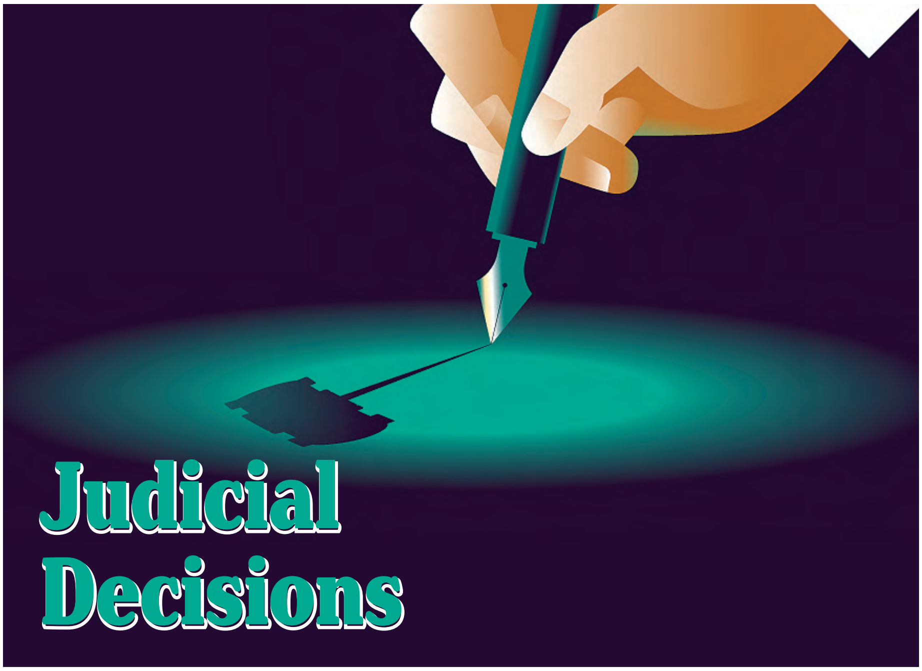
EX-OFFICIO NON-VOTING DIRECTORS
Phillip Bratton, CPP, PSP
Control Risks
Sugar Land, TX, USA

Lisa C. DuBrock, CPP
Radian Compliance
Park Ridge, IL, USA

EUROPEAN REGIONAL BOARD CHAIR
Erik de Vries, CPP, PSP
DutchRisk BV
Dinxperlo, The Netherlands

NORTH AMERICAN REGIONAL BOARD CHAIR
Mark J. Folmer, CPP, PSP
Robotic Assistance Devices
Montreal, Quebec, Canada

LATIN AMERICA CARIBBEAN REGIONAL BOARD CHAIR
Pablo Colombres, CPP
GIF International
Sao Paulo, Brazil



Judicial Decisions

Workplace safety. A U.S. federal jury found international fruit company Chiquita Brands liable for eight deaths in Colombia. The killings were carried out by a right-wing paramilitary group during an internal conflict, which began in the 1960s and resulted in the deaths of at least 220,000 people.

In 2007, Chiquita pled guilty to paying a U.S.-designated terrorist organization in Colombia in exchange for leaving banana-producing sites in two areas unharmed. The company made payments from 1997 to 2004 to the United Self-Defense Forces of Colombia (AUC), even after the United States designated the group as a Foreign Terrorist Organization (FTO) and a Specially Designated Global Terrorist (SDGT) in 2001. The designation means that financial interactions with the AUC are a criminal act.

The south Florida decision was the first verdict in many cases—which were originally filed in New Jersey—where AUC victims are seeking compensation for Chiquita's decision to continue paying the AUC. The jury ordered the company to pay $38.3 million to the surviving family members of eight AUC victims, which included farmers, trade unionists, and other civilians.

Chiquita has said it will appeal the verdict. (*John Doe 1 et al. v. Chiquita Brands International, Inc., et al.*, U.S. District Court for the District of New Jersey, No. 07-cv-03406-JAG, 2024)

Australia

Whistleblowers. The Supreme Court sentenced a former Australian Army lawyer to five years and eight months in prison for leaking information about alleged war crimes, including illegal killings, committed by Australian soldiers in Afghanistan.

David McBride, who will be eligible for parole in 2026, leaked classified military files to journalists. The information was used in a series of articles, "The Afghan Files," first published by Australian public broadcaster ABC in 2017.

McBride pled guilty to three charges, including sharing classified documents and theft, but maintained that he did not believe he was breaking the law. Justice David Mossop, however, determined that McBride lacked any display of remorse and his actions were aggravated given his high security clearance. *(The Queen v. David William McBride,* The Supreme Court of the Australian Capital Territory, No. SCC 127 of 2019, 2024)

The Netherlands

Money laundering. A panel of judges in the East Brabant District Court convicted Alexey Pertsev on money laundering charges, sentencing him to more than five years in prison.

Pertsev co-developed and founded Tornado Cash, a crypto anonymizing tool. The court found that Tornado Cash allowed criminals and terrorists to launder $1.2 billion in stolen cryptocurrency.

"Tornado Cash makes a complete anonymous deposit and withdrawal possible from Tornado Cash, thereby concealing or disguising the person who has the actual control over the cryptocurrency; in other words: who owns the cryptocurrency," the court said in a statement.

Tornado Cash and similar apps are advertised to improve the privacy of crypto users. Multiple countries sanctioned the app—including the United States—in 2022 for its involvement in laundering part of $600 million in virtual currency stolen by North Korean hackers.

In Pertsev's case, prosecutors argued that the activity went beyond the right to privacy, with Pertsev deliberately ignoring indications of criminal activity. The court determined that the platform lacked any barriers for people who wanted to use Tornado Cash for money laundering and that Pertsev knew the platform was being used for this purpose.

Along with the prison sentence, the court ruled that seized items, including a Porsche and cryptocurrency worth €1.9 million ($2.1 million), will not be returned to Pertsev. *(The Netherlands v. Alexey Pertsev,* East Brabant District Court, No. 82/198261-22, 2024)

United States

Railway safety. The U.S. Department of Justice and the Environmental Protection Agency (EPA) reached a $310 million settlement agreement with railway company Norfolk Southern for the derailment of a train in East Palestine, Ohio.

The company will pay an estimated $235 million for past and future cleanup efforts and a $15 million penalty for alleged viola-

Illustration by Iuliia Laguta

tions of the Clean Water Act, the maximum fine permitted under the law. The cleanup, which was conducted by the EPA, dealt with contaminated air, water, and soil polluted by toxic fumes from the crash.

After the train derailed on 3 February 2023, emergency responders burned five of the train cars that were carrying vinyl chloride, a carcinogenic chemical used to produce plastic, to avoid an uncontrolled explosion. However, the controlled burn created toxic fumes that spread across the area, generating concerns about long-term impacts to residents' health.

Under the settlement, Norfolk Southern agreed to pay $25 million for a 20-year community health program that will provide medical monitoring and mental health services for qualified residents and first responders. The company will also pay $15 million for long-term monitoring of groundwater and surface water for 10 years, another $15 million for private drinking well water monitoring, and an estimated $6 million for a waterways' remediation plan.

The agreement is pending final court approval. *(United States v. Norfolk Southern Railway Company,* U.S. District Court for the Northern District of Ohio Eastern Division, No. 23-cv-517, 2024)

School shooting. James and Jennifer Crumbley—the parents of the teenager who shot and killed four students in 2021 in Oxford, Michigan—were each sentenced to serve 10 to 15 years in prison.

The Crumbleys, who were tried separately, are the first parents to be held criminally responsible for a mass school shooting carried out by their child. They were found guilty of four counts of involuntary manslaughter because they failed to prevent their son from taking a firearm from their home and killing four students—Madisyn Baldwin, Tate Myre, Justin Shilling, and Hana St. Juliana—and injuring six more and a teacher. James Crumbley had bought the firearm three days before the shooting and then gifted it to his son, even though he had signed a form that said it was illegal to purchase a gun for someone else.

The shooter, Ethan, was sentenced to life in prison without parole. During his trial, he pled guilty to terrorism, four counts of first-degree murder, and 19 other related charges.

Both parents are appealing the convictions. *(People of the State of Michigan v. James Robert Crumbley,* Oakland Circuit Court, No. 2022-273389-FH, 2024; *People of the State of Michigan v. Jennifer Lynn Crumbley,* Oakland Circuit Court, No. 2022-279990-FH, 2024)

Judicial Spotlight

European Union

Privacy. The European Court of Human Rights determined that strong encryption is fundamental to the basic right of privacy.

The source of the ruling involved a 2017 incident when encrypted messaging platform Telegram was ordered by the Russian Federal Security Service to help decrypt communications of users suspected of terrorist involvement. At the time, the Russian government required Telegram and other Internet communication providers to store all communication content and data, as well as give the data and the information to decrypt it to law enforcement when ordered.

Telegram opposed the order, arguing that acquiescence would create a backdoor threatening encryption for all users. Russian courts subsequently fined the company and banned the app.

Russian citizen Anton Podchasov claimed that forced decryption of users' communications would violate their rights to a private life, which is protected in Article 8 of the European Convention of Human Rights. The court determined that forced continuous storage of communications and related data, authorities' potential access to the data, and Telegram's obligation to decrypt the data if encrypted interfered with Podchasov's Article 8 rights.

The court added that encryption helps protect people and businesses from others who would abuse information technologies, and decrypting encrypted communications could weaken encryption protections for all users.

The decision safeguards encrypted communications, giving guidance to other courts where end-to-end encryption is or will be debated. *(Podchasov v. Russia,* European Court of Human Rights, No. 33696/19, 2024)

Legislation

Czech Republic

Gun control. The Czech Parliament approved an amendment to the nation's existing Firearms Act, which closes loopholes allowing citizens to easily and legally purchase firearms.

The amendment will go into effect in 2026 and require gun sellers to report suspicious purchases. Although it will not require a psychological exam for gun license applicants, doctors—including psychiatrists—would have access to an online registry of guns and owners with the power to flag individuals buying several weapons.

Lawmakers introduced the amendment in 2017, but it stalled during the COVID-19 pandemic. Work on the proposal resumed in 2022, with the public renewing its attention to the issue in December 2023 after a graduate student with a history of depression used eight legally purchased firearms to kill 14 people and himself at Charles University in Prague.

European Union

Cyber resilience. The European Union (EU) Council and Parliament reached a provisional agreement in early March on the Cyber Solidarity Act, which will create a cybersecurity emergency system composed of national cyber hubs. These hubs will be responsible for identifying and acting on cyber threats, supporting various preparedness efforts. The legislation is pending until endorsed by the EU's Council and Parliament.

Japan

Information security. In May 2024, Japan enacted a law that creates a new system to manage who has special access to classified economic information.

The law, requires government and private sector personnel requesting access to classified information to pass a screening test, which considers criminal history, personal history, and previous experience in handling information. If approved, the security clearance is valid for 10 years.

The protected information could include details on economic sanctions, cyberattacks against critical sectors and suppliers, artificial intelligence (AI), and other technology that is under development, even in the private sector, that can be applied to the military.

The new law also mandates that anyone who leaks information critical to Japan's economic security can be sentenced to up to five years in prison or fined up to ¥5 million ($33,220).

United States

Surveillance. U.S. President Joe Biden signed legislation (HR 7888) into law that reauthorized the Foreign Intelligence Surveillance Act (FISA).

The program—which is known as Section 702 of the FISA—allows the U.S. government to collect communications of non-Americans who are outside of the United States for the purposes of gathering foreign intelligence. It does not require the government to secure a warrant for this data. U.S. officials have credited this surveillance tool with disrupting terrorist attacks and foreign espionage and with generating intelligence for specific security operations.

Regulations

Italy

Artificial intelligence. The Garante Per La Protezione (GPDP)—Italy's privacy watchdog—fined the city of Trento €50,000 ($54,225) for violating data protection rules in how it used artificial intelligence in street surveillance projects.

The GPDP also ordered the city to delete data collected as part of two scientific research projects funded by the EU. The projects attempted to find technology solutions that could improve safety in urban areas. The data collected in these efforts was shared with third parties and "the anonymization techniques used" on the data were insufficient, according to the GPDP.

Other issues with the projects included the city's failure to fully disclose the possibility of recording private conversations on public streets. ■

ADVERTISERS INDEX

Please visit our *Security Management* advertisers highlighted in orange at GSX in Orlando, Florida.

BOOTH #		PAGE #
1938	Advancis	06
2660	Altronix	13
1251	Ameristar Perimeter Security	18
1414	AXIS Communications	02
------	BLACKCLOAK	42-43
------	Brownyard Group	51
1620	CEIA USA	27
------	Control Risks	49
------	DMP	21
1588	Impact Security	35
1701	Hanwha Vision	04
1917	IDIS Americas	57
967	Liferaft Navigator	33
1039	Morse Watchmans	08
2600	NAPCO Security Technologies	68, S2, S4
2035	Par-Kut International	26
1400	Securitas Technology	11
------	Speco Technologies	41
------	StrongPoles	47
2212	Team Software	39
3015	ZBeta	16-17
EXHIBITOR MAP SPONSORS:		
2200	Allied Universal	S10-11
1474	Everon	S10-11
1259	GardaWorld	S10-11
1460	GardaWorld	S10-11
2600	GardaWorld	S10-11
675	Hexagon	S10-11
2600	Napco	S10-11
2650	Prosegur	S10-11
1055	Shooter Detection Systems	S10-11

Advancis
www.advancis.net

Altronix
ww.altronix.com

Ameristar Perimeter Security
www.ameristarperimeter.com

AXIS Communications
www.axis.com

BLACKCLOAK
www.blackcloak.io

Brownyard Group
www.brownyard.com

CEIA
www.ceia.net

Control Risks
www.controlrisks/one

DMP
www.dmp.com

Impact Security
defenselite.com

Hanwha Vision
www.hanwhavisionamerica.com

IDIS
www.idisamericas.com

Liferaft Navigator
www.liferaftinc.com

Morse Watchmans
www.morsewatchmans.com

Napco Security Technologies
www.napcosecurity.com

Par-Kut International
www.guard-booth.net

Securitas Technology
www.securitastechnology.com

Speco Technologies
www.specotech.com

StrongPoles
www.strongpoles.com

Team Software/Workwave
www.teamsoftware.com

ZBeta
www.zbeta.com

RENOVATIONS AT ROOSEVELT ISLAND

Sportspark, a community recreational facility on Roosevelt Island, New York, opened in 1977 and is operated by the Roosevelt Island Operating Corporation (RIOC). When renovations began in 2021, RIOC collaborated with technology solutions provider Elite Design Systems to implement wide area network and local area network infrastructure to improve communications and connectivity, as well as surveillance coverage that encompassed the entire island. The project covered key locations, such as a new Sportspark facility and a youth center.

MERGERS & MOVES

Thoma Bravo ⇄ Everbridge, Inc.

Thoma Bravo, a software investment firm, acquired Everbridge, which will become a privately held company.

Resideo Technologies, Inc. ⇄ Snap One Holdings Corp.

Resideo bought Snap One and will integrate Snap One into its ADI Global Distribution segment.

Vitaprotech ⇄ Identiv, Inc.

The acquisition of Identiv expands Vitaprotech's access to North American customers.

Trinity Safety Group ⇄ Caliber Safety

The acquisition will allow Trinity to solidify its presence as a safety provider in certain areas of the United States.

Award

Retailer L.L. Bean was selected as the winner of the 2024 Maine Employers' Mutual Insurance Company Award for Excellence in Safety. It was chosen for its participation in safety workshops and training programs.

Contract

The U.S. General Services Administration awarded General Dynamics Information Technology a $922 million contract to modernize Central Command's IT infrastructure.

Announcement

Physical security design and managed services firm ZBeta announced the creation of a new, manufacturer-agnostic innovation and security solution testing lab in Chicago, Illinois. The LabZ test environment will enable security professionals to collaboratively test and research new physical security solutions and services.

Partnerships

Smart Locks

Everest Infrastructure Partners and Iloq entered a partnership that will bring battery-free smart locks to U.S. telecom towers, helping protect communication infrastructure.

Inside Threat Detection

EchoMark launched its strategic partners program with the announcement of partnerships with Adaptive Integration, CBTS, ManTech, and TachTech.

Security Operations Center

HiveWatch and Verkada partnered their respective GSOC operating system and access control and video solutions.

Photo courtesy of Elite Design Systems

Where Risk Management Planning Can Help

The Current State of Security Risk Management report, published by ASIS International in June 2024 and sponsored by LifeRaft, examined the security threat landscape. The research asked which security threats presented the most risk, what threats manifested into actual significant incidents that had to be managed, and how well risk planning performed against different categories of security incidents. For more findings from this research report, visit *asisonline.org/2024-risk-management-research*

Did a Risk Management Plan Help Manage a Significant Security Incident?

48% Plan identified the threat(s) and helped manage the incident.

32% Had multiple incidents and the risk management plan helped with some but not others.

11% Plan identified the threat(s) but did not help manage the incident.

9% Plan did not help with any incidents, or they did not have a plan.

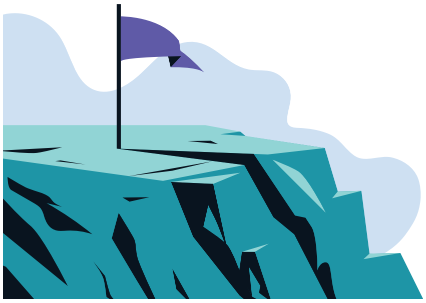
ASIS INTERNATIONAL SECURITY ISSUES RESEARCH

Sponsored by LifeRaft

Which Security Threats Pose the Most Risk to Organizations?

TOP TIER RISKS

- Workplace violence or active assailant
- Ransomware or other cyberattack



MIDDLE TIER RISKS

- Outsider property theft or destruction
- Insider property theft or destruction
- Natural disaster or climate change
- Compliance failure
- Organized crime activity
- Supply chain disruptions

LOWER TIER RISKS

- General civil unrest
- Terrorism or war
- Unrest directed at the organization
- Kidnapping, extortion, or other executive protection issues

How Many Organizations Experienced a Significant Incident*?

75% experienced at least one security-related significant incident.

18% experienced at least four different types of significant incidents.

***Significant Incident:** An incident that had a significant impact on their operations, profitability, or reputation.

Infographic design by *Security Management*, iStock

SECURITY MANAGEMENT

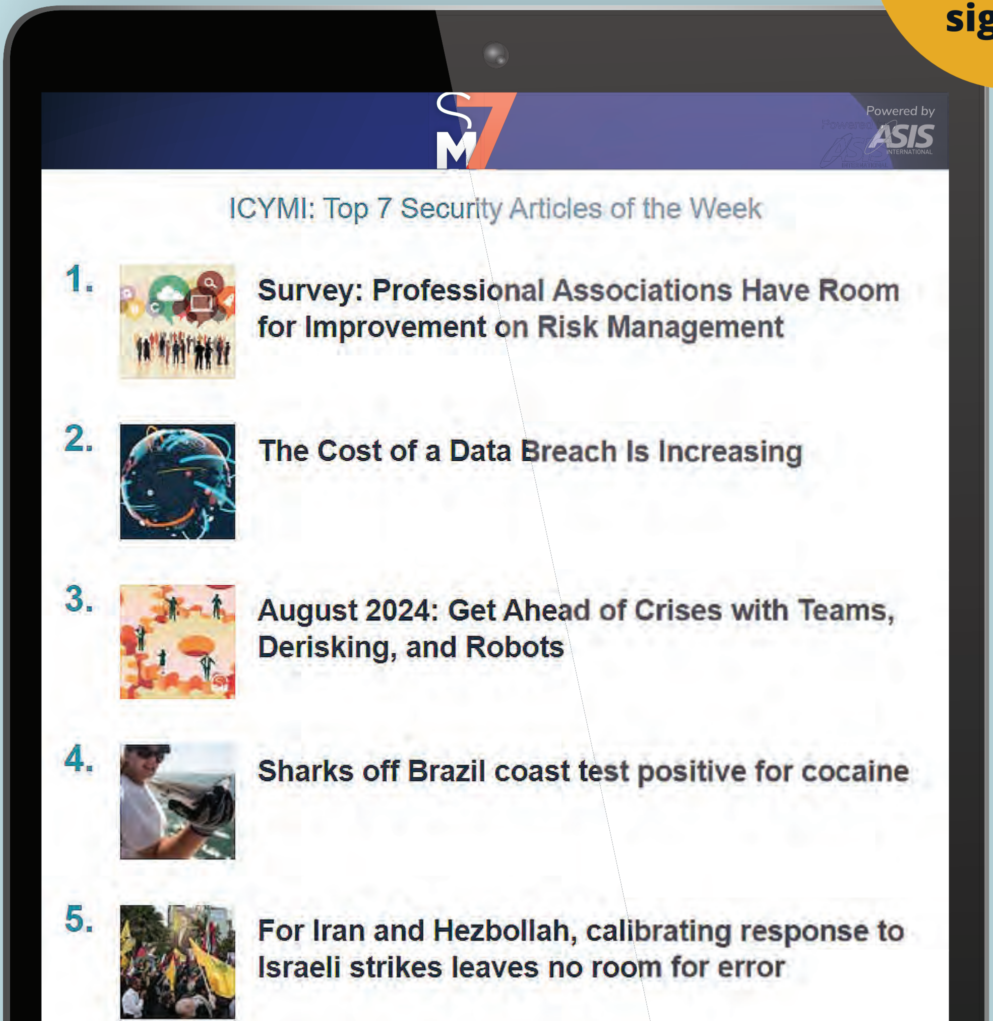
Your Security. Simplified.

Cut through the noise and stay informed with SM7.

Each week, receive a curated selection of the seven most crucial security stories you need to know. Brought to you by ASIS International, SM7 helps you stay on top of the latest developments in the security world.

Sign Up ▶

Non-ASIS members are eligible to sign up.



SM7

Powered by ASIS INTERNATIONAL

ICYMI: Top 7 Security Articles of the Week

1. Survey: Professional Associations Have Room for Improvement on Risk Management
2. The Cost of a Data Breach Is Increasing
3. August 2024: Get Ahead of Crises with Teams, Derisking, and Robots
4. Sharks off Brazil coast test positive for cocaine
5. For Iran and Hezbollah, calibrating response to Israeli strikes leaves no room for error