SECURITY MANAGEMENT
September/October 2021
Published by ASIS International

Extreme Stress

Employees are feeling burned out and could be at risk for workplace violence or disclosing sensitive information. In response, employers are offering more proactive support.

By Megan Gates

Hanwha Techwin

It's time to eXpect more from your surveillance solutions

Hanwha Techwin's new line of Wisenet X series cameras combine performance with the latest in Artificial Intelligence (AI) technology.

Unparalleled Image Quality

Next-level cybersecurity

Unprecedented Object Detection

Artificial Intelligence algorithms and Deep Learning technology filter out irrelevant movements and generate only the events you need to see, resulting in a fully secure, end-to-end workflow generating fewer false alarms and creating greater operational efficiency.

That's the power of Wisenet AI

At the "InterseXtion" of image quality, cybersecurity and AI.

GSX
GLOBAL SECURITY EXCHANGE

Visit us at Booth #1641

HanwhaSecurity.com

If Trouble Hits Your Company at 2 a.m. Who Will Respond?

If you have Prosegur's security officers, they will. If you have Prosegur's remote monitoring, the trouble can be noticed and addressed before it happens. And if you have Prosegur's risk management services, the trouble may not even happen at all.

Today security involves a 360° look at the threats you face, addressing them before they can cause damage. And this can only be achieved by incorporating people, technology and processes into an integrated security strategy that meets the challenges of 2021 and beyond.

Call us before 2 a.m.

PROSEGUR
SECURITY

(888) 808-6992
www.prosegur.us
GSX Booth #2141

For product info #2 securitymgmt.hotims.com

Contents Notable

"While much attention has been paid of late to homegrown far-right and far-left extremists, jihadist terrorism has not disappeared—it merely evolved."

Scott Stewart outlines the dramatic shifts in the terrorist landscape during the past 20 years and what they mean for security today. **Page 40**

26

The percentage of the Mexican population that may fall into poverty as a result of the COVID-19 pandemic's effect on the economy. And when poverty rises, crime often follows. **Page 54**

"Insider threat programs are not designed to call people out—they're designed to facilitate help and resources."

Rebecca Morgan, chief of the Insider Threat Division within the U.S. Defense Counterintelligence and Security Agency, explains how myriad stressors could develop insider threat risks, but proactive outreach could help. **Page 32**

"Profitability and human rights are not necessarily mutually exclusive."

Eva Nolle, CPP, examines the growing importance of corporate human rights to consumers and to courts. **Page 50**

"Not having that check-in, if people watch it and nobody does anything, can increase the trauma for the person being harassed."

Emily May, cofounder of Hollaback!, shares guidance on bystander intervention in addressing harassment. **Page 18**

98.66

The percentage increase in reports of online enticement targeting children between January and September 2020, compared to the same period in 2019, according to the U.S. National Center for Missing and Exploited Children. **Page 19**

$1.85 million

The average remediation cost of a ransomware attack in 2021, including business downtime, lost orders, and operational costs. **Page 25**

Security Management (ISSN 0145-9406) Volume 65, Number 5, is published bimonthly by ASIS International, 1625 Prince St., Alexandria, VA 22314; 703.519.6200; fax: 703.519.6299. Subscriptions: ASIS members—$60 for 1 year (included in dues, non-deductible). Nonmembers in US, Canada, and Mexico—1 year, $60; 3 years, $162. All others—air delivery—1 year, $120. Bulk subscription rates available. Periodicals postage paid at Alexandria, VA and additional mailing offices. Mailed in Canada under IPM #0743968. Postmaster: Send address changes to ASIS International, Attn: *Security Management*, 1625 Prince St., Alexandria, VA 22314. *Security Management* is a registered trademark and its use is prohibited.

Visit us at GSX
Booth 1733

It's your space.

Make sure you know when someone invades it.

SNEAK DETECTION

Our tailgate detection solution allows only one authorized person at a time. Its sleek design reduces cost and complexity versus mantraps and other devices, or it can even enhance those solutions. Your access control, made more secure—that's the Detex effect.

Call 800-729-3839 detex.com/sneak31

DETEX®

Contents Features

SEPTEMBER/OCTOBER 2021

EXECUTIVE TEAM

Peter J. O'Neil, FASAE, CAE
chief executive officer
Peter.O'Neil@asisonline.org

Nancy Green, FASAE, CAE
chief global learning
and strategy officer
Nancy.Green@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 Morelisse
Account Manager
Companies M through Z
703.518.1502
Femke.Morelisse@asisonline.org

COVER STORY

28

From Report to Support

After a year of extreme stress, employees are feeling burned out and could be at risk for workplace violence or disclosing sensitive information. In response, employers are changing their insider threat programs to offer more support.
By Megan Gates

38

TERRORISM

The Threat Remains

Jihadi terrorism organizations may have been badly disrupted in the decades after 9/11, but they continue to pose a viable threat worldwide—especially as their structure shifts to grassroots movements.
By Scott Stewart

46

DUE DILIGENCE

Bridging the Legal/Ethical Gap

Shifting regulation and decreasing consumer tolerance for corporate abuses of human rights may soon have non-compliant companies seeing both profits fall and losses in courtrooms unless they instigate a paradigm shift.
By Eva Nolle, CPP

52

GLOBAL MANAGEMENT

How Security is Changing in Latin America

Organized crime, shifting workforces, and stricter hiring requirements are influencing the role of security leaders across Latin America.
By Claire Meyer

Cover illustration by Stuart Briers

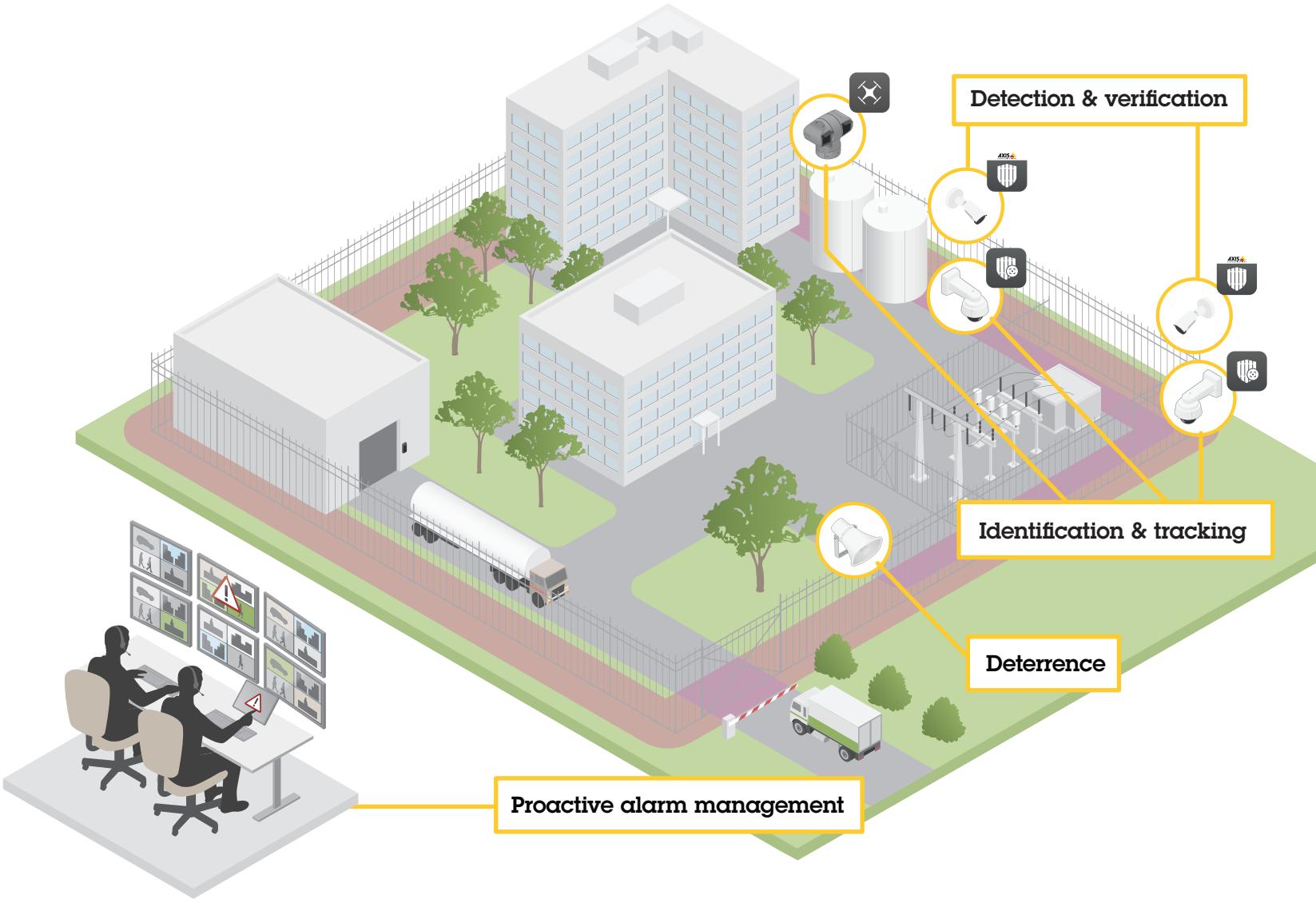
From perimeter to critical core.

Safeguard your perimeter from intrusion.

- Axis thermal cameras
- AXIS Perimeter Defender
- Axis PTZ cameras
- Video management system
- Network audio solutions
- Autotracking
- Drone detection

Protect your perimeter from intrusion – in real time – in challenging lighting or complete darkness with thermal technology and analytics. Identify intruders with automatic visual close ups with PTZ autotracking and deter with live or pre-recorded messages using horn speakers. Safeguard your air space from unwanted activity with drone detection analytics and pan, tilt and zoom cameras. Manage your security solution from your video management software - centrally or remotely.

Learn more: www.axis-communications.com/safeguard-perimeter



Contents Departments

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.

16
NEWS AND TRENDS
Tension and Intervention
As customers bristle against ongoing COVID-19 restrictions, frontline employees are at risk for pushback, harassment, and violence.
By Claire Meyer

20
CASE STUDY
Powering the Perimeter
Power provider Hydro One shifts to an incident-based solution, combining previously disparate data points to better inform security decisions.
By Sara Mosqueda

22
CYBERSECURITY
The Risk of Underwriting
With ransomware rising and data breaches increasingly commonplace, current prices for cyber insurance policies may not accurately reflect risk.
By Megan Gates

64
LEGAL REPORT
Judicial Decisions
A Wisconsin pharmacist who intentionally tampered with COVID-19 vaccine vials at his work received a three-year prison sentence.
By Sara Mosqeuda

10
Contributing Authors

12
Online Exclusives
An analysis of protests in Philadelphia resulted in key lessons for private organizations.

14
Editor's Note
"Storytelling is...what turns preparation into ritual and victims into saviors," wrote Amanda Ripley in *The Unthinkable*.

57
Security Technology
Environmental experts and security practitioners are raising the alarm on emissions-induced climate change and its effect on critical infrastructure.

59
Industry News
Changi Airport Group in Singapore will integrate its civilian airport with a unified security platform.
By Sara Mosqueda

60
ASIS News
GSX is the culmination of ASIS's core values, says ASIS President John Petruzzi, Jr., CPP.

61
ASIS Global Board of Directors

66
Marketplace

67
Advertiser Index

68
Infographic
Food shortages worldwide drove an increase of illegal, counterfeit, and potentially unsafe food onto the market in 2020.

Contributing Authors

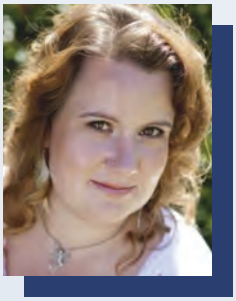
Scott Stewart

VICE PRESIDENT OF INTELLIGENCE, TORCHSTONE GLOBAL

Scott Stewart is a seasoned protective intelligence practitioner with 35 years of analytical, investigative, and security experience. Before joining TorchStone Global, Stewart led global analysis of terrorism and security topics at Stratfor from 2004 to 2020 and was the protective intelligence coordinator for Dell.

Stewart also spent 10 years as a special agent with the U.S. Department of State's Diplomatic Security Service (DSS), where he was the lead DSS investigator assigned to the 1993 World Trade Center bombing and the follow-up New York City bomb plot, among other cases.

"The Threat Remains," Page 38



Eva Nolle, CPP

PARTNER, CERAVOID

Eva Nolle, CPP, CFE (Certified Fraud Examiner), specializes in commercial intelligence, including due diligence enquiries, background screenings, political risk analysis, and commercial and fraud investigations.

During the last decade, she has helped clients operating in Africa gain a better understanding of potential risks when operating on the continent and how to avoid, mitigate, transfer, accept, or exploit them. Nolle holds a bachelor's degree in risk and security management.

"Bridging the Legal/Ethical Gap," Page 46

Yan Byalik, CPP

SECURITY ADMINISTRATOR

Yan Byalik, CPP, is the security administrator for the City of Newport News, Virginia, where he manages a team tasked with protecting the city's critical infrastructure. He serves on numerous city multidisciplinary working groups providing security input on major initiatives such as mass vaccinations, election security, and special events.

Book Review, Page 17

Mike Edgerton, CPP

MANAGER OF PORT SECURITY

Mike Edgerton, CPP, is the manager of port security for the Port Authority of New York and New Jersey, and he was previously an international port security consultant based in the Middle East. He is also a retired military officer with service in both the U.S. Coast Guard and U.S. Navy.

Book Review, Page 24

NEW FEATURE

SCENE CHANGE DETECTION

speco technologies®

Giving You More.

Alarms will be triggered if the scene of the video has been tampered with.

RECEIVE AN ALERT NOTIFICATION IF YOUR SCENE IS:

MOVED

BLURRED

VANDALIZED

COVERED

Scan to watch video

Visit **specotech.com** or call **1-800-645-5516** to learn more about this great feature!

For product info #5 securitymgmt.hotims.com

Online Exclusives

Read these articles and more online at *asisonline.org/SM-Online*

The Changed Nature of Civil Unrest

By Mark Concordia

On 30 May 2020, the first in a series of large-scale protests began in Philadelphia. Civil unrest continued during the next week. Police responses to the mass protests included the deployment of CS gas (tear gas) and rubber bullets against protestors and civilians on 52nd Street in West Philadelphia and protestors on Interstate 676. By 2 June, 692 people were arrested, 72 police vehicles were vandalized, and 104 officers were injured or assaulted. The civil unrest in Philadelphia cost more than $21 million.

It is essential to acknowledge the significant contributions and efforts of individuals and agencies across Philadelphia that responded to the civil unrest and professionally performed their duties and responsibilities in a dynamic, tense, and complex environment. Their efforts undoubtedly mitigated further violence and property damage; however, we must focus on the lessons learned from this experience if we want to prepare security operations for the new norms of civil unrest.

When Extreme Views Lead to Extreme Acts

By Steven Crimando

While diversity can strengthen an organization, strong or extreme beliefs in the workplace can be a double-edged sword. An employee's passion for a belief or cause might manifest itself as a real commitment to their employer or a project, but it can also create friction, erode workforce cohesion, and consume valuable resources when dealing with conflict.

Finding the right balance between welcoming diverse views and minimizing tension between those who hold those views and others be tricky, but it is necessary. Left unchecked, extreme beliefs not only threaten cohesion and productivity, they can also compromise safety and raise the risk of disruptive behaviors, even violence.

Extremism in Plain Sight: Recognizing Symbols and Threats

By Sheelagh Brady

We live in a visual world. According to recent research, images are central to how we interpret things, give meaning, and communicate with others. Our ability to absorb and interpret visual information is the basis of the industrial society and the information age. The meaning derived from a visual, however, is as much about the context in which we see it as it is about the image itself. Once it is removed from its original context (which is easier now because of powerful editing technology) and placed within another, it can have a multiplicity of possible new meanings, found researchers in a 2017 report, *Critical Studies on Terrorism*. Even the most definitive, universal symbol can be disconnected from its traditional meaning and appropriated for another cause.

So, what does this mean for monitoring signs of extremism in the workplace? If the meaning is not fixed, could a symbol often associated with an extremist group be entirely innocent in another context?

Engaging Employees on Their Mental Health

By Scott Briscoe

The U.S. National Safety Council (NSC) reported in May 2021 that nine in 10 employees said their workplaces caused them stress and 83 percent said they experienced "emotional exhaustion."

"Our work and our workplaces impact our mental health and wellbeing," the NSC said. "This has never been more evident than with the changes in working conditions this past year—with some working from home indefinitely, some in extraordinarily high-stress and high-risk frontline jobs, often for longer hours, and others experiencing layoffs and job insecurities. ...Mental distress includes periods of intense nervousness, hopelessness, restlessness, depression, feeling like things require great effort, or feeling worthless or down on oneself. This distress is painful and costly for both employers and employees."

Images by iStock

Learning the Red Flag Indicators of Human Trafficking in Multitenant Spaces

By Lauren R. Shapiro

Some private industries have a high potential for encountering trafficking victims or operations. Multitenant retail spaces like malls can house department stores, supermarkets, restaurants, pharmacies, and kiosks, as well as specialty stores or service providers. Private security personnel, regardless of whether they work for a specific store or for the shopping center itself, are ideally situated to observe people who are vulnerable to trafficking or are currently being trafficked.

Throughout the workday, security personnel observe people as they shop, eat, chat, work, or rest on benches. Surveillance skills used to watch and evaluate customers and employees can be instrumental in recognizing human trafficking victims.

Shifts in Safety and Critical Infrastructure

Hosted by Chuck Harold

The August 2021 episode of SM Highlights, sponsored by AlertEnterprise, features conversations with Mohammed Shehzad about managing the unique and complex nature of university security technology lifecycles and Ross Johnson, CPP, about the latest good news on the horizon about electric grid security.

Listen to the SM Highlights podcast at *asisonline.org/podcasts.*

TRENDING News & Analysis

Manchester Arena Bombing

An independent public inquiry into the mass attack at a 2017 concert in Manchester, England, found "serious shortcomings" in security.

Domestic Extremism

The Biden administration unveiled a national strategy to combat domestic extremism without adding new laws.

Propaganda and Misinformation

Terrorist organizations used the COVID-19 pandemic to exacerbate mistrust in public institutions, Europol found.

Daily news available at *asisonline.org/TodayinSecurity.*

SOCIAL MEDIA

KEEP IN TOUCH

@SecMgmtMag

@SecMgmtMag

ASIS International

RISK AND PREPARATION

"Contrary to popular expectations, this is what happens in a real disaster. Civilization holds. People move in groups whenever they can. They are usually far more polite than they are normally. They look out for one another, and they maintain hierarchies." These perhaps unexpected findings are at the core of Amanda Ripley's book *The Unthinkable: Who Survives When Disaster Strikes—and Why*. This tendency towards civility explains why people survive disasters—human kindness—and also why they perish—niceties allow people to deny reality and delay escape.

Ripley, an investigative journalist for *The Atlantic*, first published *Unthinkable* in 2008, but the book has special meaning this year—the 20th anniversary of 9/11—because a meeting with survivors inspired the book.

Preparation in the form of disaster training is critical, but convincing people of this need is difficult, Ripley wrote. "When they do have drills, most people see them as a waste of time. They overestimate how well their minds will perform in a real crisis. When the alarm goes off, they know they are being interrupted and inconvenienced, but they don't necessarily know how much they might one day appreciate the remedial help."

The best way to get the brain to perform under extreme stress is to run it through rehearsals beforehand.

GSX, which debuts virtually on 15 September and continues in both in-person and digital formats 27–29 September, provides the perfect environment to contemplate risk, preparation, and planning. Ripley will share her insights on addressing conflict at Tuesday's keynote. Find out more about other GSX events, including additional keynotes, educational sessions, and exhibits at *gsx.org*.

In *Unthinkable*, Ripley devotes her final chapter to Rick Rescorla, CPP, vice president of security for Morgan Stanley Dean Witter & Co. and ASIS member. After a 1993 bombing forced an evacuation of corporate offices at the World Trade Center in New York City, Rescorla made many changes, including frequent, all-staff fire drills. He trained people to descend the stairs two-by-two and insisted that the higher floors evacuate first—compensating for the tendency people have to become overly courteous in disasters.

"The radicalism of Rescorla's drills cannot be overstated. Remember, Morgan Stanley is an investment bank. Millionaire, high-performance bankers on the 73rd floor chafed at Rescorla's evacuation regime," Ripley wrote. "But Rescorla did it anyway. He didn't care whether he was popular. His military training had taught him a simple rule of human nature...the best way to get the brain to perform under extreme stress is to run it through rehearsals beforehand."

The training paid off. "Rescorla taught Morgan Stanley employees to save themselves," wrote Ripley. "When the tower collapsed, only 13 Morgan Stanley colleagues—including Rescorla and four of his security officers—were inside. The other 2,687 were safe."

GSX can facilitate another successful tactic through education, networking, and camaraderie after this tumultuous past year. Ripley urges all of us to "tell the story of Rick Rescorla...or your own tale of walking through hellfire. Storytelling is essential to survival. It's what turns preparation into ritual and victims into saviors." ■

Teresa Anderson
Editor-in-Chief

Illustration by iStock; *Security Management*

GAME DAY AT RECORD SPEED.

OPENGATE™ (NEW)
Groundbreaking Weapons Detection System

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

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

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

CEIA USA
WWW.CEIA-USA.COM

Tension and Intervention

Customers increasingly bristle against ongoing restrictions and mandates, leaving frontline employees at risk for pushback, harassment, and violence. Could trained bystanders' intervention diffuse the situation?

By Claire Meyer

"No." In response to new restrictions, requirements, or expectations—from COVID-19 mask mandates and social distancing to heightened demands for respect and racial equality—this simple refusal is often the spark to a larger reckoning.

Retail employees found themselves embroiled in arguments over customers' politics and beliefs about COVID-19. Asian Americans and Pacific Islanders (AAPI) faced a 149 percent rise in hate crime in the United States, according to Stop AAPI Hate, with a particular spike in verbal abuse and physical attacks. Airlines delayed a return to serving inflight alcohol given an uptick in passenger disruptions, unruly behavior, and hostility or abuse toward flight attendants—especially in response to mask mandate enforcement.

Especially during the past five years, we have seen waves of harassment against particular communities.

As a result of these tense climates, organizations are taking steps to better prepare employees for confrontation. The U.S. Transportation Security Administration (TSA) announced in June that it would restart flight attendant self-defense training to address physical altercations both on and off the aircraft.

However, a key element in flight attendants' toolkit has been recently missing. Many regular travelers are not flying due to business restrictions or other factors, so typical go-to

Illustration by *Security Management;* photos by iStock

When we speak about situational awareness to this audience, we teach them to be purposefully conscious of the two Rs: risks and resources.

helpers are missing from flights, said Sara Nelson, president of the Association of Flight Attendants-CWA, to CNBC. Those passengers understand the expectations of behavior on planes and can intervene or create peer pressure which can diffuse potential conflicts.

Frontline employees at retailers and other businesses have also faced increased conflict during the past 18 months, but their challenges with irate or offensive customers have lasted significantly longer than that. According to a *Racial Bias in Retail Study* conducted by makeup retailer Sephora, one in five retail employees reported having personally experienced unfair treatment based on their race at their workplace—either from customers or coworkers.

In response to workplace conflict, a dozen retailers—including Gap, Inc.; Dick's Sporting Goods; and Sephora—announced a new Inclusive Retail campaign that seeks to arm employees and customers with tools to ensure inclusion, safety, and acceptance of retail associates, especially since customer frustration around pandemic restrictions can manifest in racist or discriminatory ways. While the campaign is not asking customers to step in and physically stop a confrontation, it aims to provide tools for bystanders to help de-escalate situations and show support for workers.

"Across the board, we see data showing rises in harassment across all major areas," including hate crimes, microaggressions, and harassment, says Emily May, cofounder and executive director at Hollaback!, a nonprofit organization that designs and distributes bystander intervention training.

"Especially over the past five years, we have seen waves of harassment against particular communities," she adds. "What we're trying to invite people to do is, instead of looking at these as independent issues, to ally with each other across these issues and design a united front—to not just show up when your community is being harassed but when other communities are being harassed as well."

Hollaback! was founded after a study of harassment incidents found that the one common denominator that gave victims hope was when someone intervenes, May says. Recent incidents—including a rise in the rate and visibility of anti-AAPI harassment, microaggressions, and hate crimes—are indicative of larger trends across the board, and people are trying to become better allies for more vulnerable populations. This leaves them eager for potential solutions.

Intervention training is a useful tool in any company's workplace violence prevention arsenal, says Steven Crimando, principal at Behavioral Science Applications. He notes that companies with significant Asian American employee bases—particularly those in the technology sector or near cities with large Asian districts or AAPI populations—are looking to boost their offerings to help employees feel and stay safe both at work and at home.

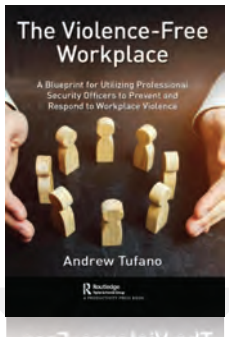
Sometimes this boost comes in the form of additional communication about existing programs such as security escorts to vehicles, incident reporting protocols, employee assistance programs, and fact sheets about crime rates and good safety practices. Companies can even leverage current investments in se-

Book Review

The Violence-Free Workplace

By Andrew Tufano. Routledge; Routledge.com; 278 pages; $49.95

The Violence-Free Workplace is an extraordinary study of what a professional security organization should look like. The author is brutally honest in analyzing the most common issues facing security organizations, from the way the industry is treated by law enforcement to the challenges it faces from its own corporate managers. The result is a thought-provoking collection of recommendations that should be reviewed and considered, even if the reader does not agree with them.



The book is well laid out and has easy to follow chapters led by a problem statement and closed out by clear-cut recommendations, plus summaries. There are numerous examples—either real or hypothetical—in every chapter that help to drive home concepts and explanations.

The book drives discussion and evaluation of the security industry. In the chapter on health and fitness standards, the author compares the discrepancy in fitness standards between security officers and lifeguards, before explaining that both positions require extended periods of stationary duty interrupted with occasional but serious high-stress activity. It becomes a fitting exclamation point to a chapter already laden with statistics on obesity by industry.

Another discussion centers on the typical use of security as either observe-and-report or forced compliance. The author delivers a compelling argument for the inadequacy of both models, considering both the need to intervene in critical incidents and the need to build and maintain positive relationships.

The discussion on key differences between law enforcement and security throughout the book is exceptional as well. The author reminds readers that when law enforcement departs after an incident, the security officer is still left at the scene dealing with long-term residual resentment from employees and friends of the person they helped remove.

Overall, this is a great book with a wealth of relevant information that would benefit not only security professionals, but also those in law enforcement who may one day work with or for a security organization. It should be shared with C-suite senior managers who may oversee their organization's security teams within their busy portfolios.

Reviewer: Yan Byalik, CPP, is the security administrator for the City of Newport News, Virginia, where he manages a team tasked with protecting the city's critical infrastructure and serves on numerous city multidisciplinary working groups providing security input on major initiatives such as mass vaccinations, election security, and special events.

curity systems—like mass notification or travel tracking programs—to establish an emergency call feature that employees can use.

After that, Crimando says organizations should ask employees what else would help them instead of guessing. The requests may be surprising—from tip lines to in-workplace bias training to self-defense courses to bystander intervention training.

"We're trying to raise the bar in terms of prevention and early recognition," Crimando says. "When we speak about situational awareness to this audience, we teach them to be purposefully conscious of the two Rs: risks and resources. The risks are the people, places, and things that may hurt us, but also in the same environment or moment, what are the people, places, and things that may help us."

Many recent incidents, especially regarding anti-Asian hate crimes in the United States, have been blitz attacks, with the assailant rushing up behind the victim. This limits the potential responses of victims and bystanders, Crimando says, so organizations could be well-served by offering tools and resources that address both pre- and post-event awareness and skills, including preventative tips that can help an individual present a less inviting target.

There are behavioral indicators of potential hostile surveillance, such as being followed or getting a gut feeling of danger, he says. Recognizing a risk early gives the person time to identify resources.

Other preventative or proactive measures can include teaching people how to walk differently and project an alert persona, emphasizing situational awareness and street-level awareness, guidance on what to do if confronted verbally, how to apply "Run. Hide. Fight." principles if necessary, managing emotional aftershocks, how to report incidents to police, and how to speak to others about the incident afterward, Crimando says.

"It's a multifactor problem, and it benefits from a multifactor approach," he adds.

Intervention training is all about giving people options, May says. While some corporate security and legal departments have balked at the idea of teaching people how to interject themselves into a potentially dangerous situation, providing choices outside of direct confrontation may create many safer avenues for bystanders.

Some schools have requested bystander intervention training for students, who are likely to intervene when they see something wrong occurring, but tend to escalate straight to direct conflict, she adds. Training helps students to see that other options could be more supportive for the victim and safer for the bystander.

Conflict de-escalation is "Gandhi-level hard" May says, differentiating it from verbal intervention. De-escalation usually requires someone in a position of authority to intervene in a potentially violent situation by observing, breathing, then connecting with the aggressor. This requires a high degree of self-control and emotional intelligence in addition to training.

Bystander intervention is more user-friendly, she adds, and Hollaback! teaches a 5D approach, which can apply to online harassment, as well as in-person incidents.

Distract. The bystander can create a distraction—whether starting a conversation with the person being harassed or simply dropping a coffee cup—to change the energy of a situation or alert the harasser that others are nearby. Online, people have taken over incendiary hashtags on Twitter with off-topic memes or GIFs to drown out hurtful commentary.

Delegate. Bystanders can ask for help, whether from an authority figure like a bus driver or police officer or another bystander. Delegating responsibility also helps to support the bystander, especially when his or her personal safety could be at risk.

Document. Bystanders can record or document an event via smartphone camera in-person, or online they could take screenshots and track hyperlinks before the offender deletes them, either to report the offense to the platform or to offer the material to the victim to use as evidence if they choose to pursue further action.

Delay. This intervention largely occurs after an incident. "Sometimes harassment is quick, and a check-in of 'I saw that; it wasn't okay. What do you need right now?' can be huge," May says. "Not having that check-in, if people watch it and nobody does anything, can increase the trauma for the person being harassed."

Direct. At first glance, people equate bystander intervention with direct action, but there are many options within this concept. Bystanders are not expected to educate the offender about their conduct, May says, but "we're merely asking you to set that boundary: 'She looks really uncomfortable, why don't you give her some space.' Once you set that boundary, turn your attention to the person being harassed."

May recommends placing heavy emphasis on personal safety—there are frequently valid reasons not to intervene, including fear for individual safety or fear of escalating the situation. But multiple options within the 5Ds are nonconfrontational and even familiar to many people; delegation can be as simple as reporting an incident of harassment to security personnel—something that many employees are already conditioned to do. The options also give people permission to intervene in more incidents, including those that involve microaggressions or other offenses that may have been hurtful to the victim but may not be strictly illegal or against company policies.

Companies can provide ongoing resources and communication about available support programs, ingraining safety into their corporate culture to help foster a community-like environment where people seek to take care of each other, May says.

"People feel more safe at work now," says Crimando. "It's the risk in between the threshold of the home to the threshold of the workplace that is concerning."

Feeling the Pandemic Pressure

More than 40 percent of employees across the world say they experienced a record high of negative emotions in 2020.

43% of employees said they experienced stress during a lot of the previous day

24% of employees said they experienced anger during a lot of the previous day

Source: *State of the Global Workplace: 2021 Report,* Gallup, July 2021

COVID Effects Let Trafficking Flourish

"COVID-19 generated conditions that increased the number of people who experienced vulnerabilities to human trafficking and interrupted existing and planned anti-trafficking conventions," according to the U.S. State Department's annual *Trafficking in Persons Report*, released in July.

Government resources worldwide were diverted from human trafficking missions to combat the coronavirus pandemic, the report said, leaving wide gaps for traffickers to target at-risk populations. School closures left children without access to education, shelter, or food. Young girls in poor or rural areas of India and Nepal were expected to leave school to help support their families, and some were forced into marriage or child labor. Elsewhere, some landlords forced their tenants to have sex with them when they could not pay rent.

"Low-wage and migrant workers, and those in the informal economy, faced riskier employment conditions, including restricted movement, minimal oversight mechanisms, withheld wages, and increasing debts—all indicators or flags for human trafficking," the report said.

Pandemic-related lockdowns forced many people to turn online for interaction, including human traffickers. The report found that online recruitment and grooming spiked as children spent more time online. The U.S. National Center for Missing and Exploited Children reported a 98.66 percent increase in online enticement reports between January and September 2020 compared to the same period in 2019.

COVID-19 affected trafficking survivors as well. A survey by the Office of Security and Cooperation in Europe (OSCE) and UN Women found that nearly 70 percent of human trafficking survivors from 35 countries reported that their financial well-being was heavily affected by COVID-19, and more than two-thirds said their mental health had declined due to government-imposed lockdowns triggering memories of past exploitation.

Pandemic-related lockdowns forced many people to turn online for interaction, including human traffickers.

The survey also noted that survivors' access to employment during the pandemic decreased by 85 percent, medical services by 73 percent, social services by 70 percent, legal assistance and access to food and water by 66 percent, psychological assistance by 64 percent, and access to safe accommodation by 63 percent.

Although government funding and attention was diverted elsewhere during the pandemic, anti-trafficking initiatives continued and evolved, the report found. Creative uses of technology—including WhatsApp forums, webinars, and online collaboration groups—enabled civil society organizations to share resources and guidance, identify victims, and expand access to training. ■

Powering the Perimeter

To improve its physical security systems and meet international regulations, power provider Hydro One shifted to a solution that combined previously disparate data points.

By Sara Mosqueda

We were looking to modernize the infrastructure in a way that will help us protect the communities that we operate in.

As the largest electricity transmission and distribution provider in Ontario, Canada, Hydro One Limited has a lot of ground to cover.

More than 110 years ago, the Legislative Assembly of Ontario approved the Power Commission Act, providing for the creation of the Hydro-Electric Power Commission of Ontario—a publicly owned power utility for the province. The electrical generation and distribution company was later broken into five different businesses in 1998, when legislators approved the Energy Competition Act. Out of those businesses, Hydro One emerged.

Today, Hydro One distributes electricity to roughly 1.4 million residential and business customers, many of them rural, accounting for 98 percent of the province's transmission capacity. Included in this coverage is power generation and distribution to 22 remote communities in the northern region of Ontario.

The power provider is in the process of making various investments in its electric transmission systems throughout the province. As the company made plans to update components of the grid, it also looked at improving other assets, including its physical and cyber perimeter defenses. Enhancing perimeter security would help protect not only an asset for the communities it serves but also the 8,700 employees that build and maintain the system.

"Prior to the upgrade itself, Hydro One's physical security system was nearing end of life and was non-integrated, predominantly an analog-based physical security system," says Ben Blakely, chief security officer and vice president of security operations for Hydro One.

Blakely adds that while the legacy systems included proprietary access control, the lack of integration meant that it was separate from video, intrusion detection, and intercom systems in Hydro One's facilities, forming gaps in situational awareness.

While the previous program could use several data points to trigger incident alarms, the unintegrated state of the system meant experienced operators with a comprehensive understanding of the individual systems and the company's standard operating procedures had to interpret the information to effectively respond to one or more alarms. All of these factors could potentially slow and complicate incident response.

"We were looking to modernize the infrastructure in a way that will help us protect the communities that we operate in. Should there be events, we need to adequately respond, and

Illustration by iStock, *Security Management*

The data that's pulled from across the field is generated through a unified security system that provides line of sight into the performance of the system.

put the right protections in place to secure our infrastructure in…those communities we operate in," Blakely says.

Besides a search for a more efficient and intelligent system, another reason Hydro One was looking to move on from the older systems was because of newer requirements levied by the North American Electric Reliability Corporation (NERC)—a not-for-profit international regulatory body that crafts and enforces reliability standards for power companies, users, and grids throughout Canada, the United States, and the northern region of Baja California, Mexico.

Essentially, the company needed to ensure that physical security systems would be effectively installed, monitored, and maintained.

Hydro One landed on a Genetec solution partly because the Canada-based corporation was already familiar to the transmission company, having worked together on previous technology projects.

It also didn't hurt that the Genetec Security Center's centralized monitoring format allowed Hydro One to encourage proper incident management and a more proactive approach to security.

With the solution's open architecture and various technology partnerships, Hydro One was able to combine input from across all other security components, from overarching programs, plans, technologies, and processes to more granular elements, such as perimeter alarms, surveillance cameras, and check-in points. Leveraging Hydro One's existing security elements lessened the financial lift for the company, and it used some new Genetec devices and applications to integrate into the updated system.

Blakely adds that a significant benefit of working with Genetec, including using the company's Mission Control system, was that it gave Hydro One access to a large channel partner community, which could help streamline the integration and installation process.

Given the scale of the project, a multiphase format was used to integrate the solution, while ensuring that customers would only experience minimum service interruptions. Establishing a preproduction environment allowed installers to test the solution and work out any kinks before taking it online.

"By taking that staged approach, rolling it… to production, allowed us to reduce risk and manage those broader business concerns," Blakely says.

"It offers a single unified platform to manage all aspects of our physical security system, with a strong component of cybersecurity, which I think everybody understands is a fairly significant risk that many of our organizations are managing," Blakely says.

Cybersecurity breaches are a rising risk for organizations that rely on computer systems. As a power transmission system, however, physical protection of its assets will always be a top concern for Hydro One—especially given the breadth of both the network and the customer base.

The system helps the organization keep tabs on activity along a spread-out infrastructure footprint. Hydro One maintains approximately 124,000 circuit kilometers of low voltage power lines, making the Security Center product useful for remotely monitoring alarms set up along the network.

Meanwhile, monitoring access safeguards the security of the power grid and local communities, helping minimize theft and vandalism, discouraging sabotage, and deterring other kinds of harmful activity. The use of Genetec Mission Control in the company's security operations center (SOC) helps ensure consistency in response management, essentially reducing the overall risk for Hydro One.

For example, the system gave Blakely's team the ability to shift from the previous format of individual alarm management—where multiple alarms or indicators related to a single event were investigated as separate incidents—to a more proactive, overarching approach to incident response.

Following the integration, when a physical access breach is detected by perimeter alarms or indicators it is displayed to an operator in the SOC. All related information is funneled from numerous sources into a visual site plan, including relevant video feeds and priority alarms. After analysis of the feeds or other alarms to determine the nature and other details of the breach, an operator is empowered to notify local police about the intrusion or take other appropriate action to address the situation.

"The data that's pulled from across the field is generated through a unified security system that provides line of sight into the performance of the system, events that are happening across the field, and allows us to respond appropriately and deploy resources to those key areas," Blakely says.

Combining physical and cybersecurity fronts with advanced reporting features provides the company with an improved quality of data from the system. With the solution, Hydro One can better analyze system performance and trends, triaging to determine if equipment or a component of the infrastructure will likely soon need fixing or replacing.

The holistic project has taken multiple years to integrate and implement, but Blakely says the final phases will be completed by the end of 2021. ■

For more information about Genetec, contact Greg Kemper at *Gkemper@genetec.com.*

The Risk of Underwriting

With ransomware increasingly commonplace, more organizations are looking into purchasing cyber insurance. But current prices for cyber policies may not accurately reflect risk.

By Megan Gates

The average cost of recovering from a ransomware attack is now 10 times the size of the ransom payment.

Who does an insurer turn to when its own systems are compromised? That question came to mind in September 2020 when insurance provider and risk management firm Arthur J. Gallagher & Co. disclosed to the U.S. Securities and Exchange Commission (SEC) that it had detected ransomware in its systems.

"We promptly took all of our global systems offline as a precautionary measure, initiated response protocols, launched an investigation, engaged the services of external cybersecurity and forensics professionals, and implemented our business continuity plans to minimize disruption to our customers," the company said in its filing to the SEC—made 48 hours after detection of the attack. "As of the date hereof, we have restarted or are in the process of restarting most of our business systems. Although we are in the early stages of assessing the incident, based on the information currently known, we do not expect the incident to have a material impact on our business, operations, or financial condition."

While the firm recovered from the event, it noted in a February 2021 filing with the SEC that cyberattacks and other incidents—including ransomware attacks—could impact future financial results.

"In the future, any material cybersecurity or data incidents, or media reports of the same, even if untrue, could cause us to experience reputational harm, loss of clients and revenue, loss of proprietary data, regulatory actions and scrutiny, sanctions or other statutory penalties, litigation, liability for failure to safeguard clients' information or financial losses," the filing explained. "Such incidents could result in confidential, personal, or proprietary information being lost or stolen, used to perpetuate fraud, maliciously made public, surreptitiously modified, or rendered inaccessible for a period of time. As we experienced in connection with the 2020 ransomware incident referred to above, during a cyberattack we might have to take our systems offline, which could interfere with services to our clients or damage our reputation. Such losses may not be insured against or not fully covered through insurance we maintain."

The questions of what is covered under cyber insurance policies, what is not, and who has coverage to begin with are increasingly coming into play as cyber incidents continue to rise—including ones targeting the insurance sector.

For instance, in May 2021 Bloomberg reported that CNA Financial Corp.—one of the

Illustration by Steve McCracken

comnet
Communication Networks

The Shortest Distance Between Two Points

Audio, Video, Data, and Ethernet Transmission Solutions

ComNet is Your Solution for Fiber Optic, Copper, and Wireless Transmission

Your transmission challenge has always been getting your audio, video, data and ethernet signals from here to there.

ComNet offers the most comprehensive line of products designed to solve every transmission challenge.

MADE IN THE USA LIFETIME WARRANTY

RAZBERI – SIMPLE, SECURE VIDEO SURVEILLANCE AND IOT SOLUTIONS

Now part of ComNet

Simple-to-deploy, manage and cybersecure video surveillance systems and IoT devices

ComNet's Razberi line provides video server appliances, combined with cybersecurity and health management software to customers worldwide. We save customers install and maintenance costs and reduce the likelihood of a costly cyber breach.

comnet

an ACRE brand

View the Full Product Line at **comnet.net** and Identify the Fiber Optic, Copper or Wireless Connectivity Solution for your Application

Contact the ComNet Design Center Now for Free Design Assistance.

Call **1-888-678-9427** or **1-203-796-5300**
or email **designcenter@comnet.net**

Visit www.comnet.net Email info@comnet.net Phone 1-203-796-5300 Toll Free 1-888-678-9427

largest insurance companies in the United States—allegedly paid $40 million to hackers to restore its networks after a ransomware incident. CNA reportedly made the payment roughly two weeks after its network was compromised and company data was stolen.

This payment occurred while the cyber insurance market is experiencing a bit of turmoil. Analysis by Marsh McLennan, the largest commercial insurance broker of U.S. business based on revenues, found that clients' cyber insurance take-up rates increased from 26 percent in 2016 to 47 percent in 2020. It saw the most interest from the education and healthcare sectors, as well as hospitality, retail, and manufacturing.

This uptick came after a series of high-profile data breaches in 2015—Anthem, Premera Blue Cross, Ashley Madison, and the U.S. Office of Personnel Management, says Mike Karbassi, chief underwriting officer for Corvus Insurance.

Karbassi adds that during this timeframe, insurance policies evolved to include cyber extortion, data recovery, business interruption, contingent business interruption, and cybercrime.

"This expanded on the traditional coverages related to data breach investigation and response costs, as well as privacy liability, regulatory and PCI fines, and penalties," he says. "At the time, coverages related to contingent system failure, hardware replacement, bodily injury, and voluntary network shutdown were typically not included, but they have emerged in the past two years."

Insurer appetite and capacity for underwriting cyber risk has contracted more recently, especially in certain high-risk industry sectors.

But all things are not looking up for the market, according to a report by the U.S. Government Accountability Office (GAO) published in May 2021.

"Despite the upward trend in take-up rates to date, insurer appetite and capacity for underwriting cyber risk has contracted more recently, especially in certain high-risk industry sectors such as healthcare and education and for public-sector entities," the GAO wrote after analyzing information from The Council of Insurance Agents and Brokers, Marsh McLennan, and AM Best. "These sources noted the contraction has resulted from factors that include increasing losses from cyberattacks, the threat of future attacks, and overall insurance market conditions."

John Pendleton, GAO director of the financial markets and community investment team, says that when GAO was conducting its five-month assessment of the cyber insurance market in the United States, it noticed that premiums for policies began increasing in 2020 and that providers were narrowing their policies.

For instance, many began crafting standalone cyber policies for clients instead of including cyber coverage in an existing policy. These policies generally combine cyber coverage with professional liability coverage. Sources that the GAO spoke to said the increase in cyber-specific policies might be the result of a desire for clarity and coverage of losses from confidentiality, integrity, or availability of data and systems. These standalone policies might also reduce lawsuits in the wake of a cyberattack and provide policyholders with higher cyber-specific limits.

"What we saw were prices were going up... take-up rates were going up, everything was drifting upwards," Pendleton says. "And insurers were getting more specific in what they were covering."

For instance, GAO found that insurance underwriters were "more carefully scrutinizing"

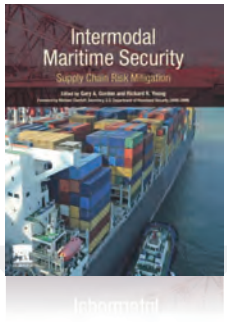
Book Review

Intermodal Maritime Security

Edited by Gary Gordon and Richard Young. Elsevier; Elsevier.com; 400 pages; $94.50

Maritime security has garnered attention in recent years as a result of reporting on the effects of piracy, cyberattacks, and even the challenges of the COVID-19 pandemic. Regardless, the complexity and importance of maritime shipping and port operations remain a mystery to many people not involved in the industry.

This book provides an excellent overview of the enormous challenges faced by the industry in the maritime supply chain and its connections to other modes of transportation. Both editors and the contributing authors have excellent academic credentials and have clearly carried out extensive research into the field. The book is written for U.S. audiences with many references to U.S. regulations and standards, but it may be of use to international practitioners as well.



Intermodal Maritime Security provides an extensive overview of the components of the maritime transportation system, the factors that affect its security, and commercial drivers. Of note is the detailed description of the components of the maritime supply chain. Initial discussions of enterprise risk also recognize the myriad drivers in ports and shipping, including financial, regulatory, and broader geopolitical concerns. These are important in the inherently competitive and multinational world of shipping that is often overlooked when addressing security concerns.

The book's strengths are in the sections on overall maritime transportation system and the regulatory regimes and programs, as well as related cybersecurity concerns, but it could have benefited from more coverage of operational technologies along with a discussion about ports' tendency to adopt a single window system for data submission and the associated risks.

In discussions of risk, there is a broad description of existing approaches to risk assessment and management with a recommendation that the U.S. Department of Defense's CARVER model be adopted for the maritime domain.

This book is well worth the investment for those who are interested in the increasingly complex field of supply chain security and how the security of ports and shipping both affect and are affected by this dynamic field.

Reviewer: Mike Edgerton, CPP, is the manager of port security for the Port Authority of New York and New Jersey, and he was previously an international port security consultant based in the Middle East. He is also a retired military officer with service in both the U.S. Coast Guard and U.S. Navy.

risks by entities that could affect future insurance availability and affordability.

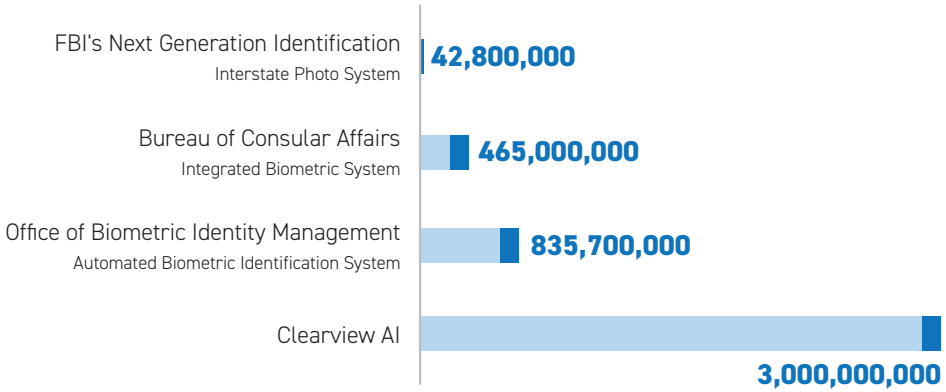
"They noted that insurers have become more selective in extending coverage to high-risk entities and industries and increasing prices of coverage they offer," the report said. "This caution has been in response to the increasing frequency, severity, and cost of cyberattacks and uncertainty about the type, scope, and targets of future attacks."

In 2020 and the beginning of 2021, organizations were repeatedly infected with ransomware. Threat actors also increased the likelihood that ransoms would be paid by threatening to publish sensitive corporate information if the victim did not pay the ransom. This occurred while the average cost of remediating a ransomware attack more than doubled, according to *The State of Ransomware 2021* global survey from Sophos.

"Remediation costs, including business downtime, lost orders, operational costs, and more, grew from an average of $761,106 in 2020 to $1.85 million in 2021," the survey assessed.

Facial Recognition

Of the facial recognition technology systems used by U.S. federal agencies for law enforcement, Clearview AI has the most photos.



Source: *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks*, U.S. Government Accountability Office, June 2021

"This means that the average cost of recovering from a ransomware attack is now 10 times the size of the ransom payment, on average."

The survey also found that the number of organizations that paid a ransom increased from 26 percent in 2020 to 32 percent in 2021; however, less than 10 percent got all their data back.

Included in these costs, ironically, are likely cyber insurance premium increases, according to consulting firm Deloitte.

"There is little public data available on actual premium increases following cyberattacks," Deloitte said in a CFO fact sheet. "Deloitte conducted informal research among leading providers of cyber insurance and found that it is not uncommon for a policyholder to face a 200 percent increase in premiums for the same coverage, or possibly even be denied coverage until stringent conditions are met following a cyber incident."

In the GAO's assessment, it found that insurance brokers expect premium increases in 2021 for larger high-risk industries. Many have also begun to reduce coverage for ransomware and higher risk sectors, like healthcare and education.

"Policies have evolved in the COVID-19 era, but likely not because of the pandemic so much as the increased frequency and severity of ransomware claims," Karbassi says. "Insurers experienced tough losses over the past year and a half, and are starting to make adjustments beyond rate increases to their policy forms."

In some instances, these adjustments include co-insurance or sub-limits on ransomware coverage. Underwriters have also started requiring that cyber insurance applicants confirm robust IT security protections exist prior to binding coverage, such as multi-factor authentication usage, email filtering tools, and a comprehensive network redundancy strategy.

"Industry participants have noted that insurers have been tightening policy terms and conditions for cyber-specific policies," the GAO wrote. "They also have been adding exclusions to traditional lines of coverage and package policies with cyber endorsements to avoid any ambiguity that coverages would overlap with cyber policies. These restrictions seek to eliminate coverage of 'silent' cyber risks that could damage multiple businesses and result in insurers accumulating significant unforeseen losses that could pose a risk to their solvency."

The average cost of recovering from a ransomware attack is now 10 times the size of the ransom payment, on average.

Also posing a challenge for insurers is the lack of data that could be used for risk forecasting and modeling. This is partly because cyber is still a young area for insurance coverage, but also because there are often few—if any—reporting requirements for cyber incidents, which prevents insurers from developing a database of historical incidents to analyze.

"In addition, a 2020 report by the International Association of Insurance Supervisors noted that incomplete or inaccurate historical data on cyber incidents decreases the reliability of actuarial models, leading to increases in uncertainty around loss estimates," the GAO wrote. "Without access to such data, some industry participants and researchers are concerned that current prices for cyber policies may not accurately reflect risk."

At Corvus, for instance, Karbassi says the firm's data science and engineering teams have created a scan that looks for vulnerabilities in a potential account's external IT infrastructure. The scan results are then used to generate a score so underwriters can assess the account.

"The scan looks at obvious aspects, such as the company's public-facing website, as well as less obvious ones, such as vulnerabilities in bits of software embedded in a company's Web applications, or unused domains owned by the company," he explains.

There are some initiatives underway to address the industrywide dearth of data, including a recommendation by the U.S. Cyberspace Solarium Commission to have Congress create an entity to understand cyber risk and help insurers craft better risk models.

The recommendation, however, had not been translated into legislation as of *Security Management's* press time. ■

Protect the everyday.

Genetec™

See us at Booth 841

For product info #13 securitymgmt.hotims.com

From Report

Illustration by Stuart Briers

to support

By Megan Gates

After a year of extreme stress, employees are feeling burned out and could be at risk for workplace violence or disclosing sensitive information. In response, employers are changing their insider threat programs to offer more support.

TRANSPORTATION IS A CRITICAL COMPONENT of modern life, and the ability to get people and goods from one location to another is essential. The Santa Clara Valley Transportation Authority (VTA) provides bus, light rail, and paratransit services for a region of Northern California that is home to Silicon Valley.

Its more than 2,000 employees continued to report to work throughout the unprecedented challenges of 2020, helping customers get to where they needed to be and providing essential services to transit-dependent and disabled individuals who rely on the system for groceries, access to doctor's appointments, and more.

And then, tragedy struck at work. Samuel Cassidy, 57, went to an early morning union meeting at one of the system's light-rail maintenance yards on 27 May 2021 and opened fire. He killed eight of his coworkers before dying by suicide as police arrived on the scene. A later investigation would find that Cassidy was unhappy with his work and held numerous grievances toward his employer and colleagues.

Evelynn Tran, interim VTA general manager and general counsel, wrote in a statement that she was struck by the courage that VTA employees had shown throughout the pandemic and in the immediate aftermath of the shooting but said that more must be done to support them. That included making VTA employees the top priority by shutting down the light rail system.

"At this point, it is impossible to estimate when service can be restored," she wrote. "There are many factors involved in restoring service, most importantly the human factor."

The incident was the third workplace shooting in less than two months in 2021 in the United States, a higher number than previous years based on analysis by the Associated Press, *USA Today*, and Northeastern University. Their analysis found that the United States averages roughly one workplace mass shooting per year. Mass shootings are defined as shootings where four or more people were killed.

These incidents represent some of the most catastrophic damage that an insider can do to his or her organization. Other incidents can range from assaults to intellectual property theft to disclosure of corporate secrets, leaving physical, reputational, and emotional damage in their wake.

Insider threat incidents are more common than one might think. A recent assessment by the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) found that more than 2 million people report some type of workplace violence each year,

with approximately 25 percent of workplace violence going unreported.

Additionally, 90 percent of cybersecurity professionals believe their organizations are vulnerable to insider threats, which cost a median of $4.45 million to recover from and take 314 days to identify and contain, according to CISA.

And the reasons why an insider might be compelled to lash out at work have been exacerbated by the COVID-19 pandemic.

"This has been a unique risk environment, and it's continuing," says Rebecca Morgan, chief of the Insider Threat Division at the Center for Development of Security Excellence, part of the Defense Counterintelligence and Security Agency (DCSA). "We have a risk environment where we have an incredibly stressed-out workforce, people are dealing with financial insecurity, medical and mental health isolation, and then trying to get a mission accomplished at the same time."

A recent employee survey from Gallup found that 45 percent of people said their own life had been affected "a lot" by the COVID-19 pandemic and that only 20 percent of employees were engaged at work.

"In addition, Gallup has found that roughly seven in 10 employees are struggling or suffering, rather than thriving, in their overall lives," wrote Jim Clifton, Gallup chairman and CEO, in the *State of the Global Workforce: 2021 Report*. "Eighty percent are not engaged or are actively disengaged at work."

The findings reflect a trend that Gallup has been tracking for the past decade: negative emotions are on the rise, and employee mental health may get worse. Unfortunately, many organizations lack data on employee wellbeing, burnout, or resiliency.

"Measuring employee mental health is critical. Besides destroying lives, suffering can destroy the human spirit that drives innovation, economic energy, and eventually, good jobs," Clifton added.

It can also create a dynamic where employees may leave—sometimes in mass numbers. A Microsoft survey of 30,000 global workers found that more than 41 percent were considering quitting or changing their profession. Additionally, 4 million Americans quit their jobs in April 2021 alone, marking the biggest spike of resignations in U.S. employment history.

"There are a number of reasons people are seeking a change, in what some economists have dubbed the 'Great Resignation,'" according to the BBC. "For some workers, the pandemic precipitated a shift in priorities, encouraging them to pursue a 'dream job,' or transition to being a stay-at-home parent. But for many, many others, the decision to leave came as a result of the way their employer treated them during the pandemic."

All of this—combined with many workforces moving out of corporate offices and into home offices—created a perfect storm where insider threats can thrive. "And we know, unequivocally, that our adversaries are prepared to take advantage of these situations and exploit them," Morgan adds.

A Prevention Paradigm Shift

In 2010, WikiLeaks published a trove of classified documents about the Iraq and Afghanistan wars—including a video of a helicopter crew opening fire on a group of people, two of whom were Reuters news agency employees.

Its source? U.S. Army intelligence analyst Chelsea Manning, who downloaded U.S. military reports onto her personal laptop and provided them to WikiLeaks. She had learned about the organization during a security training course she attended while in the Army.

In an interview with *The New York Times* after then-U.S. President Barack Obama commuted her prison sentence, Manning said that she was initially intrigued by the work that WikiLeaks was doing and wanted Americans to see what was happening in the Middle East as she saw it.

Months later, after WikiLeaks published the leaked materials, Manning was arrested, court martialed, and sentenced to 35 years in prison. It was a personal reckoning for her, but also for how the U.S. government addresses insider threats—especially since it came on the heels of an active shooter incident at Fort Hood when U.S. Army Major and Medical Corps psychiatrist Nidal Hasan killed 13 people and injured more than 30 others.

In October 2011, Obama signed an executive order creating the National Insider

The Power of Hello

Organizations, especially critical infrastructure ones, face a variety of threats from internal and external actors. Combatting these threats can be complicated, but it can also start with a simple step of saying "hello," according to the U.S. Cybersecurity and Infrastructure Security Agency (CISA).

"Used effectively, the right words can be a powerful tool," CISA says. "Simply saying 'Hello' can prompt a casual conversation with unknown individuals and help you determine why they are there."

CISA recommends using the OHNO approach: Observe, Initiate a Hello, Navigate the Risk, and Obtain Help. This can help employees observe, evaluate suspicious behaviors, and empower them to mitigate potential risk or obtain help when necessary.

For more information on the OHNO approach, visit CISA's dedicated Web page: *www.cisa.gov/employee-vigilance-power-hello.*

Photos by iStock

Threat Task Force (NITTF) to deter, detect, and mitigate actions by employees who may represent a threat to national security. The order instructed the NITTF to develop a national insider threat program with supporting policy, standards, guidance, and training under the guidance of the U.S. attorney general and the director of national intelligence.

The NITTF was designed to create a new paradigm in addressing insider threats. Originally, the U.S. government took a more traditional law enforcement approach to insider threat detection and management, essentially addressing the risk only after an incident, Morgan says.

"In many cases, there were precursors of behavior that, if identified and addressed, might have prevented the loss of insider information or—in some cases—tragedy," she says. "The new policy mandated that insider threat be managed in a proactive manner by a team that adds in human resources folks, employee assistance, mental health and behavioral, legal counsel, and cybersecurity."

Creating this type of team recognized that insider threats may have malicious intent—seeking to harm the organization or coworkers—or they could be individuals who need help and are looking for their employer to step in to provide it.

"We have invested a tremendous amount in our national security workforce, and it is in everyone's interest to help someone who may feel he or she has no other option than to commit an egregious act—such as espionage, unauthorized disclosure, suicide, workplace violence, or sabotage," according to an NITTF fact sheet.

A crucial component of insider threat prevention, mitigation, and response is understanding the human factor—what an employee's baseline of normal is and when that individual is deviating from it.

"These programs are designed to help folks," Morgan says. "We like to use the phrase, 'Turning people around, not turning them in.' Our goal is to get ahead of any negative action."

Achieving this goal requires having an insider threat program in place; an awareness strategy to share information with the entire workforce on the risk, indicators of a potential problem, and how to report them; and then a method to address reports quickly. It also includes reassessing communication strategies and support for the workforce, such as sharing information on mental health and other employee support resources during the COVID-19 pandemic.

"One of the things we put out, beginning around spring 2020 and then going into summer, was resources on personal resilience," Morgan explains. "It encouraged insiders to harden the target, make themselves aware of their susceptibility, and giving them tools to facilitate their own mental health and wellness while reinforcing the idea that it's okay to struggle."

At the same time, Morgan's former director, Bill Evanina, and then Michael Orlando, acting director of national intelligence, released memos clarifying that people would

not lose their clearances for minor financial issues, seeking mental health counseling, or asking for support.

"We want folks to get help," Morgan says. "2020 was a horrible year for everyone, but any given year someone in your staff is having a terrible time or a crisis; they're going through a divorce, etc. Insider threat programs are not designed to call people out—they're designed to facilitate help and resources."

Outside the House

If you can't break into a building yourself, one of the best ways to obtain access is to recruit someone who already has a key. Recruitment of insiders to provide information on their employers or share government secrets is nothing new.

"There are also unwitting insiders who can be exploited by others," the NITTF fact sheet said. "Our adversaries have become increasingly sophisticated in targeting U.S. interests, and an individual may be deceived into advancing our adversaries' objectives without knowingly doing so."

For instance, Jon Ford, managing director at Mandiant who works with government agencies and corporations on insider threat and risk management, has seen a trend develop since 2020 where threat actor groups from foreign countries target employees at organizations to recruit them to provide sensitive information—sometimes even unwittingly, such as an employee accidentally opening an email attachment that is then used to launch a corporate espionage attack.

"In the last 90 days, we've notified 15 organizations that eastern European groups were looking to recruit individuals to specific companies and were advertising that they would welcome their support and pay for their access into those systems," Ford tells *Security Management* in a May 2021 interview. "We were able to notify these companies—some of which were clients."

External threat actors, especially nation states, have been conducting campaigns, with a particular interest in medical research. This includes COVID-19 research, as well as cancer and other major disease research initiatives that were underway before the pandemic. Insiders committed 59 percent of healthcare data breaches, with another 4 percent involving partners with authorized access, according to the 2021 *Verizon Data Breach Investigations Report (DBIR)*. Broadly speaking, external threat actors outpaced internal actors in 2021, Verizon found, with external actors responsible for 61 percent of breaches while the remaining 39 percent were because of an internal actor.

"The insider breaches that were maliciously motivated have not shown up in the top three patterns in healthcare for the past several years," wrote the authors of Verizon's 2021 *DBIR*. "But does this mean they are no longer occurring, or are they still around but we just aren't catching them (like Bigfoot)? Only time will tell."

In acknowledgement of this threat, the Center for Development of Security Excellence released an implementation guide for insider risk programs for the healthcare and public health sector in August 2020.

One concerning trend is for threat actors to recruit an individual in an IT administration or security role who has a working knowledge of the technology controls in place to detect and monitor insider activity.

"We've done responses to organizations where an individual in IT actually suppressed alerts to ensure their activity was not flagged further up," says Ford, whose background is in investigating insider threats for the FBI. "One individual was stealing millions (of dollars); another person was stealing intellectual property."

In another incident, a client asked Ford and his team to assess a situation where executives believed an external hacker had gained access to their organization. After a review, Ford says they determined it was actually two of the client's contractors who "believed they were smarter than they company they worked for, and wanted to prove it," Ford says. "They started calling in bomb threats, which led to evacuation of buildings. It got out of hand for what they intended."

Threats like this show that while having technological resources in place to detect and monitor network activity is beneficial, they are not enough to stop insider threats.

"For insider threat, there is not a technology solution that's holistic," Ford says. "If you're going to have a full insider threat program, it's complementary to the technology. It has to consider people, processes, and tools."

More Help

Since the executive order creating the NITTF was rolled out in 2011, Morgan says the U.S. federal government has been successful at establishing an insider threat program that closely mirrors the federal policy guidelines. It also worked to promote best practices to the private sector, primarily in the critical infrastructure space that is largely owned and operated by private organizations.

"We've tried to pause and come together to identify the reasons for these policies and bring awareness to the general public by demystifying insider risk programs," she adds. "People, in the past, have perceived them as big brotherish—someone is watching you all the time."

Instead, Morgan says it's important to explain why insider threat programs exist and use them to identify risky individual behav-

Avoid Predictable Post-Occupancy Program Drift

Learn how centralizing systems management and maintenance post - occupancy can dramatically improve security program integrity and return on investment over time.

Secure your tomorrow.

Extraordinary efforts go into implementing security systems effectively on day one - installed per standard, compliant with security policy, and fully operable and functional. See how to avoid the untold amounts of damage that are subsequently done to these efforts over time through successive service calls, moves, adds, and changes. Sites deviate, policy compliance wanders, consistency suffers and operational budgets are squandered.

Download the case study: zbeta.com/drift

ZBETA

ior and organizational culture that could increase the threat.

"Sometimes it's poor management or lack of transparency or toxicity in the workplace," she says. "We work with organizations to remediate those items."

Understanding workplace dynamics and being culturally competent play a role in mitigating insider threats. This is one of the reasons that the NITTF created the theme of "Cultural Awareness and Insider Threat" for September's National Insider Threat Awareness Month (NITAM).

"A culturally competent organization has the capacity to introduce and integrate various cultures or subcultures in order to produce better outcomes and enhance operational effectiveness," according to the Center for Development of Security Excellence's *Understanding the Intersection of Cultural Competence and Organizational Risk*. "In the context of insider risk, better outcomes and enhanced operational effectiveness can be measured by the successful prevention, detection, deterrence, and mitigation of the potential insider threat in all of its manifestations: cyber threats, espionage, fraud, sabotage, trade secret theft, unauthorized disclosure, mishandling classified information, and kinetic violence."

Highlighted as a sub-theme this year is the risk of toxic workplaces and leaders—such as individuals who put their own needs or image above their subordinates, micromanagers, or insecure leaders.

"This type of leadership can perpetuate a toxic work environment, and is often marked by poor communication, constant stress, regular infighting, mental or physical abuse, and stressed relationships amongst coworkers," according to a NITAM stakeholder communications guide. Also highlighted are top–down culture, microaggressions in the workplace, and work–life stressors.

Identifying these elements in the workplace and working to reduce or eliminate them can proactively lower insider threat risks, the Center for Development of Security Excellence has found.

"Insiders at risk of causing harm to themselves, harm to others, or damage to their organizations often display concerning behaviors that result from a combination of personal predispositions and an inability to cope with life stressors," according to the center's report. "These stressors that are frequently generated in the workplace can be caused by a hostile, toxic, and harmful work culture. Certain organizational cultures may cause or intensify stressors for members of its community and increase the risk of a potential threat. If this risk is not mitigated, then it can lead to exceptionally grave damage."

In response to the rise in workplace physical violence, CISA has also crafted a de-escalation series for insider threat that complements its existing *Insider Threat Mitigation Guide*, says Susan Schneider, active assailant security branch chief at CISA. As of *Security Management's* press time, CISA planned to release the de-escalation series during the third quarter of 2021.

Many critical infrastructure owners and operators that CISA works with began asking for resources on de-escalation and intervention strategies as they implemented their insider threat plans.

Schneider says CISA looked at an existing de-escalation training created by the Oakland Public Library system, which has nine techniques for employees to use when interacting with an unruly or upset visitor or colleague. CISA also looked at techniques used in healthcare for calming down agitated patients.

"We did not want it to be a law enforcement approach," Schneider says. "We wanted it to be from a space where anyone can de-escalate a situation—calming the situation by talking to an individual."

Engaging people and talking to them is not only a good security strategy that lets someone know you're aware of their presence, but also beneficial for building a good organizational culture where people can share their stressors and feel supported by their colleagues.

"I may have a bad day and spout off about how bad it's going to be, but that day doesn't mean I'm going to go down the path of violence," Schneider says. "The good thing about the remote work environment is it forces you to talk to individuals and have team meetings. Communication is better, and people will share with you so you can determine what their baseline of behavior is." ■

Megan Gates is senior editor for *Security Management*. Connect with her at *megan.gates@asisonline.org*. Follow her on Twitter: *@mgngates*.

What is Cultural Competence?

Having a culturally competent workplace can play a large role in mitigating the risk of insider threats. But what does that actually mean? The Center for Development of Security Excellence highlights these characteristics:

Valuing and adapting to diversity and the cultural context of the community

Managing dynamics of difference

Acquiring and institutionalizing cultural knowledge

Conducting self-assessment of behaviors, attitudes, and policies that enable effective cross-cultural work

Involving key stakeholders and the community

Source: *Cultural Competence and Insider Risk*, Center for Development of Security Excellence, 2021

SIX LEARNING THEATERS.
COUNTLESS INSIGHTS.

We're excited to announce the Global Security Exchange (GSX) 2021 learning theater themes, designed to help you address not only security's most pressing topics and issues, but your own as a professional—whether you join in person or digitally.

Defensive Strategies:
Surviving the Unexpected
Emergency Preparedness
• Insider Threat • Risk Management
Live On Site | ● Live Broadcast

Game Plans:
What's Next for Security
Post Pandemic • New Normal
• Organizational Management
Live On Site | On-Demand

Offensive Strategies:
Preparing for an Attack
Business Continuity • Resilience
• Mitigation Measures
Live On Site | ● Live Broadcast

Highlight Reel:
Best Practices
Case Studies • Lessons Learned
• Newsworthy
Live On Site | On-Demand

Future Plays:
Navigate the Changing Landscape
Cybersecurity Trends • Technology
• Digital Transformation
Live On Site | On-Demand

Coaching:
Building and Motivating Teams
Leadership • Talent Development
• DE&I
Live On Site | On-Demand

GSX
GLOBAL SECURITY EXCHANGE

27-29 SEPTEMBER 2021
ORLANDO, FL, USA | ONLINE

REGISTER NOW AT GSX.ORG/LEARNING

SECURITY MANAGEMENT

Wherever You Are

It's never been easier to access the vital knowledge you need to stay on the forefront of the security profession.

Receive timely information on emerging security threats and practical solutions through the channels that best fit your schedule and career.

MAGAZINE

Read the award-winning print publication from ASIS International.

WEB

Enjoy the latest news and a responsive design that looks great on your smartphone or tablet.

SOCIAL

Join the discussion on Facebook and Twitter.

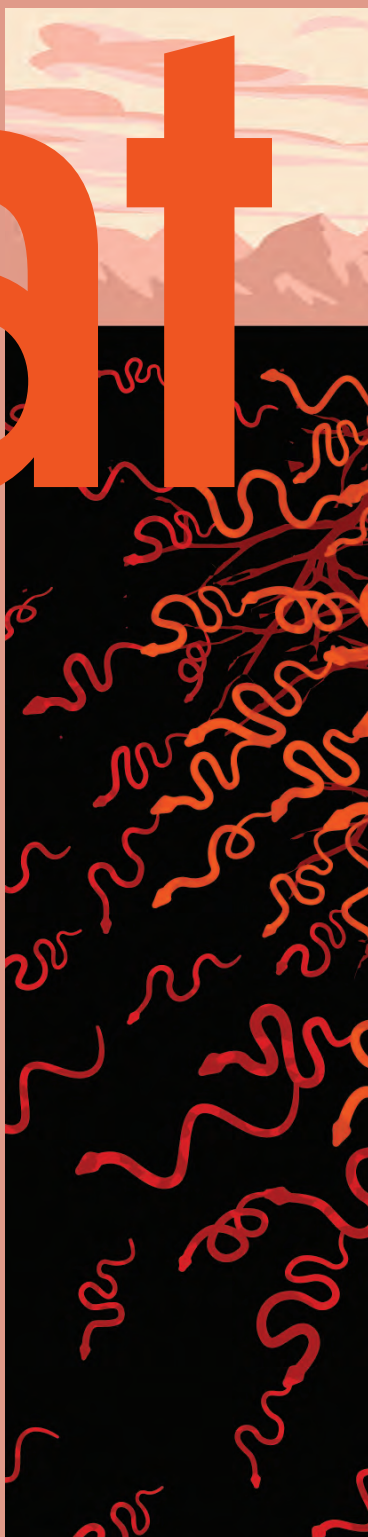
PODCAST

Hear what security professionals are talking about.

EMAIL

Subscribe to the *SM Daily* and Deep Dive eNewsletters.

the threat remains



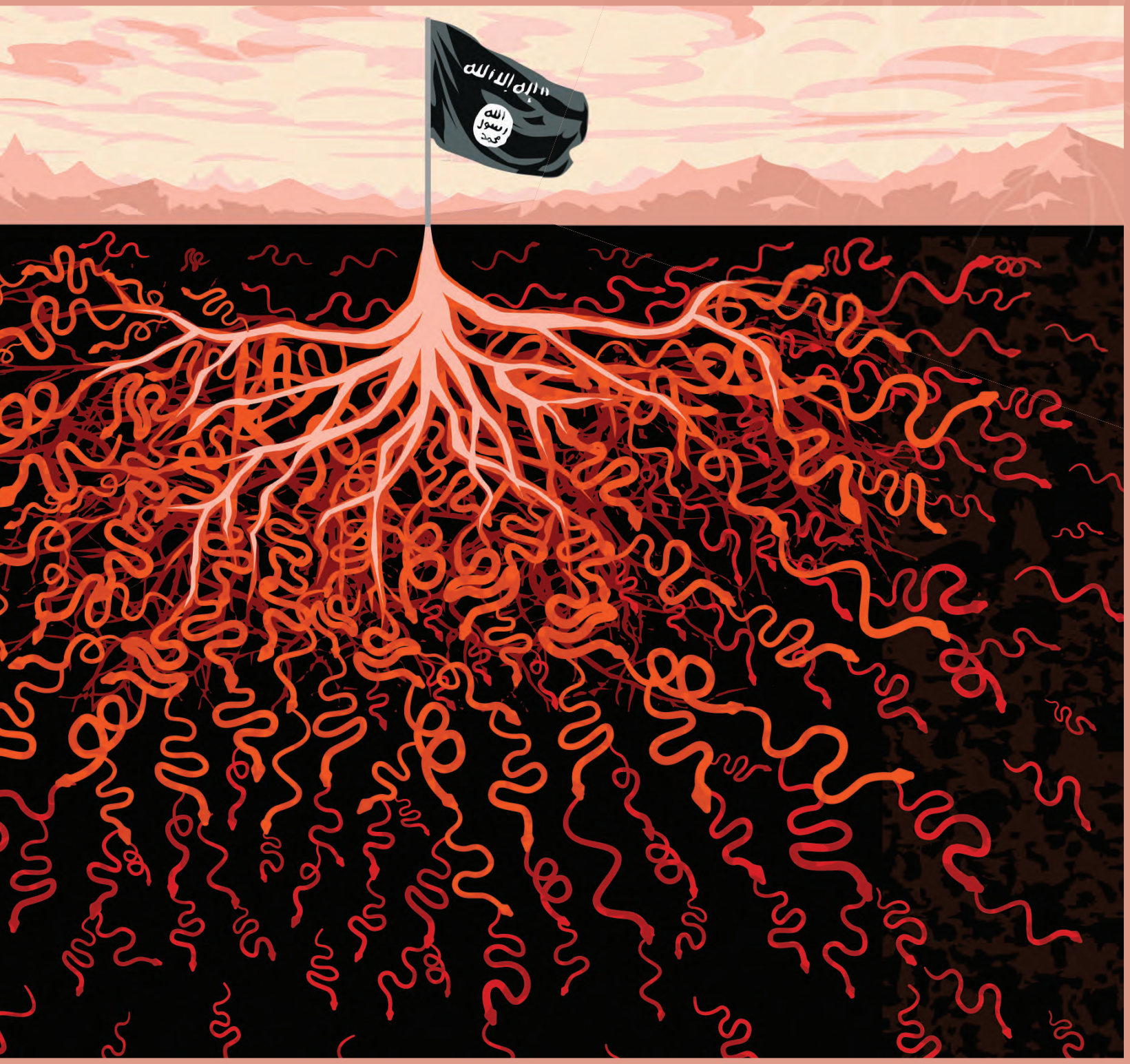
Jihadi terrorism organizations may have been badly disrupted in the decades after 9/11, but they continue to pose a viable threat worldwide—especially as their structure shifts to grassroots movements.

By Scott Stewart

On 11 September 2001, a group of operatives dispatched by al Qaeda leadership hijacked four planes and conducted a series of attacks targeting symbols of America's economy, military, and government. Although passengers on one of the planes heroically diverted it from the intended target of the U.S. Capitol by crashing it in a Pennsylvania field, the successful attacks against the World Trade Center and the Pentagon shook the United States—and the world—to the core.

The 9/11 attacks—and the oft-repeated threats by al Qaeda to conduct subsequent attacks—sparked a visceral U.S. response that led to the invasion of Afghanistan in 2001, the invasion of Iraq in 2003, and a wide-ranging global war on terror that resulted in American military and intelligence activity in scores of countries around the world. Some estimate that since 2001, the war on terror has cost the United States $6.4 trillion.

Illustration by Daniel Hertzberg


لا إله إلا الله
الله
رسول
محمد

Anniversaries, whether personal or public, are often a time to reflect on what has happened, and to ponder what the future may bring. While much attention has been paid of late to homegrown far-right and far-left extremists, jihadist terrorism has not disappeared—it merely evolved. So, as the world marks the 20th anniversary of the 9/11 attacks, it behooves security professionals to take stock of the jihadist movement today, forecast where the movement is headed, and consider the implications of ongoing terrorist activity.

Defining the Movement

Before one can properly gauge the status of the jihadist movement, it is necessary to define it. Jihadism is an ideological movement through which militant Islamists seek to establish a global Islamic polity via jihad. While jihad simply means "struggle" in Arabic, when used in this context, militant Islamists are clearly referring to an armed struggle or, as some have termed it, a "holy war." Thus, jihadists are those who seek to topple current regimes through armed struggle and replace them with an Islamic government run in accordance with their austere interpretation of Islam.

Modern jihadism is not a monolith. It has always been a movement composed of a variety of distinct groups and individuals. For example, al Qaeda leader Osama bin Laden's famous 1998 "Declaration of War against the Jews and Crusaders" was not only signed by bin Laden, but also by Ayman al-Zawahiri (leader of the Egyptian Islamic Jihad), Refa'i Ahmed Taha Musa (leader of the Egyptian Islamic Group), Shaykh Mir Hamzah (secretary of the Jamiat Ulema-e-Pakistan), and Fazlur Rahman (leader of the jihad movement of Bangladesh).

Following the 9/11 attacks and the tremendous amount of publicity they generated, that notoriety helped al Qaeda quickly rise to the forefront of the global jihadist movement, leading many other jihadist groups and individuals to swear allegiance to bin Laden. Some did this out of sincere admiration, while others did it more pragmatically to capitalize on al Qaeda's fame to help recruit fighters and raise funds to support their own local struggles.

> Despite setbacks and disruptions, al Qaeda has adapted and survived.

Al Qaeda's rise to prominence resulted in the group evolving from a small vanguard group into a much larger, though loosely organized, network composed of three distinct components: bin Laden and the core al Qaeda group; other franchise jihadist groups that pledged allegiance to bin Laden and assumed the al Qaeda mantle; and individual grassroots jihadists inspired by al Qaeda but not formally a member of the core or a franchise group.

Some of the al Qaeda franchise groups were closer than others to the core group in terms of personal relationships, ideology, and military doctrine. Among the groups that maintained close links with bin Laden and the core leadership were the jihadists in Yemen and Saudi Arabia who would later form al Qaeda in the Arabian Peninsula (AQAP).

The relationships with other franchise groups were fraught and less collaborative. For example, the tension between al Qaeda and Abu Musab al-Zarqawi's Jama'at al-Tawhid wal-Jihad (Organization for Monotheism and Jihad or JNIM) over both ideology and military doctrine resurfaced repeatedly, even after al-Zarqawi pledged allegiance to bin Laden and changed his group's name to al Qaeda in the Land of the Two Rivers (also known as al Qaeda in Iraq or AQI).

These tensions would later boil over and lead to AQI's successor group, the Islamic State in Iraq and al Sham (ISIS), breaking away

Selected Timeline of Jihadist Attacks/Events Since 2001

AQ: al Qaeda-affiliated **IS**: Islamic State-affiliated *:Grassroots, inspired, funded, or trained by the related group

- October 2002 — Bali bombings (AQ)
- May 2003 — Casablanca bombings (AQ)
- November 2003 — Istanbul truck bombings (AQ)
- March 2004 — Madrid train bombings (AQ)
- July 2005 — London transit bombings (AQ*)
- January 2007 — Algerian Salafist Group for Preaching and Combat becomes al Qaeda in the Arabian Peninsula
- September 2008 — Islamabad Marriott bombing (AQ)
- January 2009 — Al Qaeda in the Arabian Peninsula formed

from al Qaeda in 2013—two years after the death of Osama bin Laden. The new group referred to itself simply as the Islamic State, and due to its successes on the battlefield in Iraq and Syria, it quickly rose in prominence and became a second powerful pole within the jihadist movement.

The Islamic State also attracted an array of franchise groups and grassroots jihadists to its orbit. Many of the Islamic State franchise groups had formerly been al Qaeda franchise groups, such as Ansar Beit al-Maqdis in Egypt, which became known as the Islamic State's Sinai Province. Other Islamic State franchises were formed by splinters that broke away from powerful al Qaeda franchise groups in places like Yemen and Somalia. Boko Haram in Nigeria, another Islamic State franchise, had previously attempted to formally join al Qaeda, but its entreaty was rejected by bin Laden and the al Qaeda core leadership due to their indiscriminate targeting of civilians and the mercurial nature of the group's leadership. It later became the Islamic State West Africa Province—a franchise of ISIS.

The Current State of al Qaeda

While al Qaeda was able to surprise the U.S. government on 9/11, after those attacks every government agency focused on the group and al Qaeda's core leadership has been under incredible pressure. The United States and its allies have pursued al Qaeda leaders across the globe, capturing some key leaders and killing a significant number of others. Efforts to neutralize the al Qaeda core leadership have even included going after those seeking refuge in sanctuaries such as Pakistan, Syria, and Iran.

In addition to capturing and killing leaders, the efforts to counter al Qaeda also concentrated on its finances, logistics, communications, and travel. This made it far more difficult for al Qaeda leaders and their terrorist operatives to function, and al Qaeda was never able to launch its long-threatened follow-up attack to 9/11.

The Islamic State's 2013 defection hurt al Qaeda both in terms of image and operations. The damage was compounded by the fact that al Qaeda was still attempting to recover from the loss of the charismatic and famous bin Laden in 2011. Newly established Islamic State franchise groups began to compete with al Qaeda franchises for manpower, finances, and territory. In several places—including Syria, Yemen, Mali, and Somalia—this competition led to open warfare.

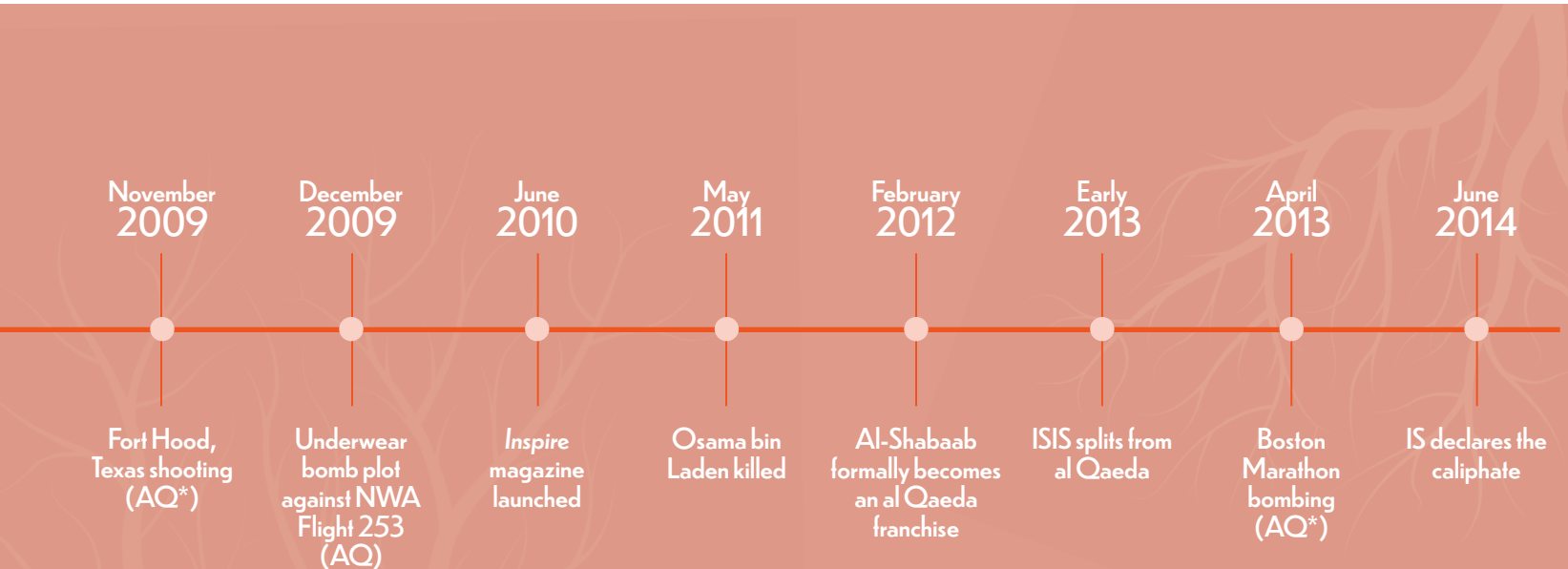
Al Qaeda's leaders must take extreme measures to stay hidden, both from Western forces and jihadist competitors, and this impacts their ability to communicate, travel, and interact with other members of the core, as well as the franchise groups.

Despite setbacks and disruptions, al Qaeda has adapted and survived. Due to the addition of franchise groups to its ranks, the Council on Foreign Relations found that the al Qaeda network has more fighters under its banner today (more than 40,000 by some counts) than the core group did prior to September 2001, when it consisted of only a few hundred jihadists.

Based upon the experience of al Qaeda franchises in failed attempts to establish jihadist states in Iraq (2006), Yemen (2011 and 2015), and Mali (2012), the al Qaeda leadership learned that it is very difficult to impose jihadist rule on people who are not ready and willing to accept it. Because of this, they have adopted a more gradualist approach to establishing Islamist rule that requires a period of ideological preaching and preparation.

Under this approach, it is important for the jihadists to become closely integrated with the local population to gain influence. Because of this, the al Qaeda core and al Qaeda franchise groups have adapted their strategy and devote the bulk of their efforts to preaching and local integration, rather than focusing large amounts of resources on planning and executing attacks against the United States and the West. This change of strategy was also influenced by the difficulty al Qaeda has had in getting operatives to the West to conduct attacks.

In recent years, groups such as Al-Shabaab in Somalia and JNIM in Mali have attempted some external attacks and regional attacks focused on Westerners, but the bulk of al Qaeda franchise group efforts remain focused locally. AQAP was very involved in fomenting



and conducting attacks attempting to target the United States, such as the attempt to bomb Northwest Airlines Flight 253 in 2009 and the printer cartridge bomb plot in 2010. But after suffering a series of devastating leadership losses in 2015 and 2016, AQAP was forced to redirect its focus to local jihad.

Today, the main threat posed by the al Qaeda pole of the jihadist movement outside of its primary areas of operation stems from grassroots jihadists who think globally but act locally, posing a far larger threat to the institutions and people of the countries its franchise groups are based in than to the West. In places like Somalia and Mali, al Qaeda franchise groups operate as insurgents that exert influence and control over large expanses of territory and the population that lives there. They attack the military and government to make their areas of operation ungovernable and thus more susceptible to their influence. They also seek to undercut anything that promotes stability or provides tax revenue to the government, so they attack business interests, tourist sites, and NGOs.

These groups also pose a persistent terrorist threat to the regions surrounding their primary areas of operation. For example, al-Shabaab has conducted terrorist attacks in Kenya and Uganda, and JNIM has conducted attacks in Ivory Coast.

The Current State of the Islamic State

After splitting from al Qaeda in 2013 and experiencing a series of dramatic battlefield victories in Syria and Iraq, the Islamic State of Iraq and al Sham declared in late June 2014 that it was establishing a global Islamic caliphate and renamed itself the Islamic State (IS). The group declared its leader, Abu Bakr al-Baghdadi, the Caliph—supreme global leader of all Muslims. Accordingly, al-Baghdadi demanded that all Muslims pledge allegiance to him, including all jihadists and jihadist groups. Many did so, which resulted in a period of dramatic growth of the Islamic State pole of the movement. The result was the creation of a global jihadist network that rivaled al Qaeda.

At the zenith of its power, the U.S.-led coalition fighting the IS estimated the group controlled some 30 percent of Syria and 40 percent of Iraq, including the cities of Mosul, Iraq, and Raqqa, Syria. They posed a direct threat to the governments of those two countries and the surrounding regions.

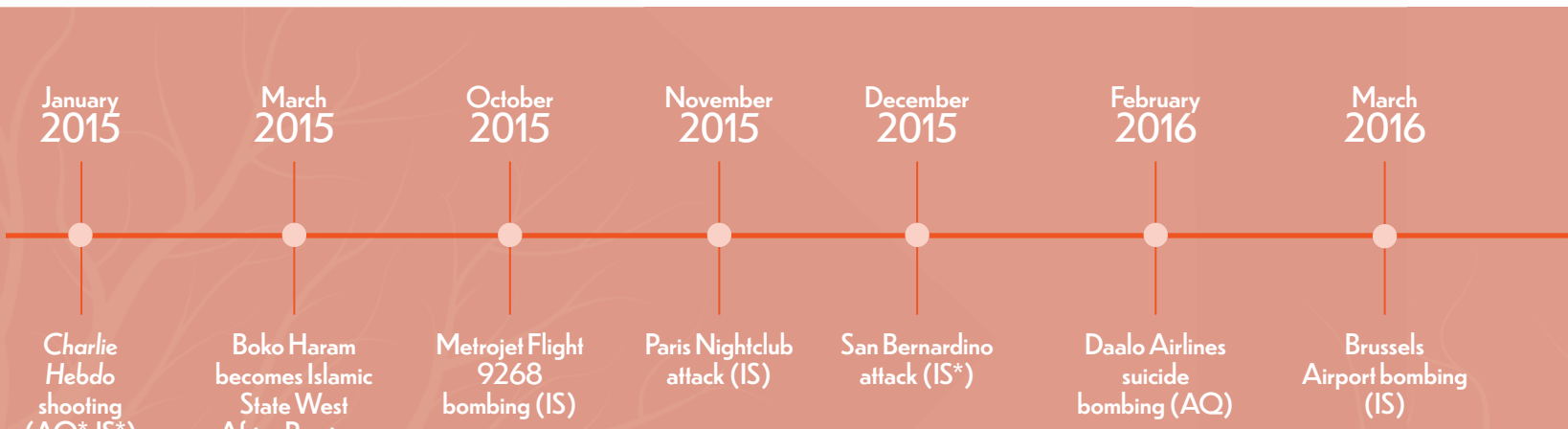
This threat brought IS to the attention of the rest of the world, and in June 2014 an American-led coalition of countries launched Operation Inherent Resolve (OIR) in Iraq to blunt the Islamic State's offensive operations. In September 2014, OIR was expanded to Syria, and within a few months, the intense campaign of airstrikes coupled with local ground forces destroyed much of the Islamic State's heavy weapons systems, targeted its economic system, and forced IS to go on the defensive.

By December 2017, the IS core had lost 95 percent of its once expansive proto-state, including Raqqa. On 27 October 2019, al-Baghdadi was killed after fleeing to Syria's Idlib province. Today, the IS core is only a shadow of what it was in mid-2014 in terms of manpower, weaponry, and money. It does however retain the potential to conduct terrorist attacks, as well as hit-and-run insurgent attacks in Syria and Iraq.

The weakened IS core is in much the same condition as its predecessor organization, the Islamic State in Iraq, was in 2010. But just as the Islamic State in Iraq was able to rebound dramatically from 2011 to 2014 and eventually conquer large portions of Syria and Iraq, so the IS core could once again grow into a powerful force if it is provided the opportunity to recover and regroup.

In terms of franchise groups, which the Islamic State calls provinces, the IS core often provides direct financial support, weapons, and operational guidance. For example, the Islamic State franchises in Libya received considerable support from the core, including foreign fighters, money, and weapons. This support allowed a Libyan franchise to assert control over the city of Sirte and proclaim an Islamic polity there until it was uprooted by Libyan ground forces strongly supported by U.S. and allied airstrikes in December 2016.

Financial support from the IS core also played a critical role in providing IS supporters in Southeast Asia with the resources needed to seize the city of Marawi in the Philippines in May 2017. After a protracted and destructive battle, the country's military reestablished control of Marawi in October 2017. Islamic State supporters had made a dramatic statement by seizing the city, but they paid a terrible price and lost a considerable number of fighters.



In areas where they must compete with stronger al Qaeda franchise groups, such as Somalia, Yemen, or Mali, the Islamic State's provinces have struggled to gain much momentum. However, in areas where they faced no significant jihadist competition, the IS franchise groups are faring better. The franchises in Mozambique and Nigeria are among the most active IS franchises in 2021.

In August 2020, the Islamic State Central Africa Province seized the port of Mocimboa da Praia in Mozambique, which it still controls as of July 2021. In March 2021, the group sent hundreds of fighters to seize Palma, a key site for Mozambique's offshore energy projects. While they only held Palma for 10 days, the seizure caused the French energy company Total to declare force majeure and suspend its operations, a move that has the potential to cost the government of Mozambique billions of dollars in lost energy royalties.

> Today, the Islamic State core is only a shadow of what it was in mid-2014 in terms of manpower, weaponry, and money.

In northeastern Nigeria, the Islamic State West Africa Province—formerly known as Boko Haram—waged a brutal and bloody insurgency that the United Nations estimates has resulted in some 300,000 deaths in Nigeria. That violence has also spilled over into nearby Cameroon, Chad, and Niger.

Both of these African franchises pose a significant insurgent and terrorist threat to governments in the region, as well as to businesses and NGOs operating there. Although they do not yet pose a global threat, they could evolve into the role if their growth is left unchecked.

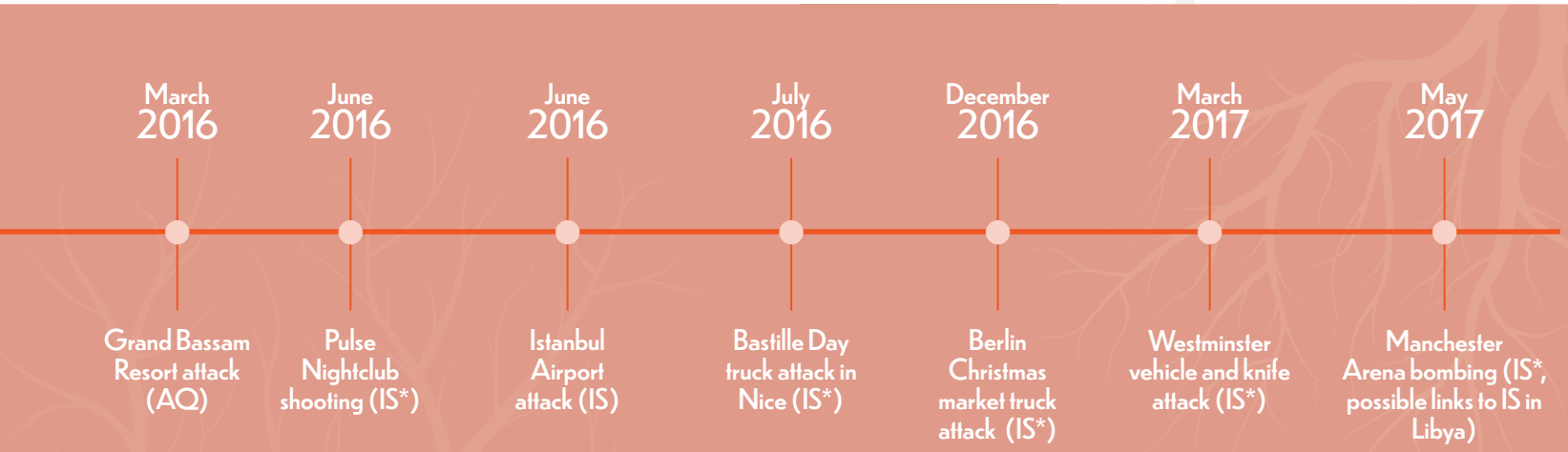
The IS core dispatched a cell of operatives to Europe to carry out terrorist attacks in 2015. Members of the cell traveled to Europe by hiding among the heavy flow of refugees from Syria's civil war. Using skills they were taught by the Islamic State and funds the organization provided, the cell conducted a series of suicide bombings and armed assaults in Paris on 13 November 2015 that targeted the national stadium, restaurants, and a nightclub—killing 132 people. Members of the cell fled France and regrouped in Brussels to conduct a suicide attack targeting Zaventem International Airport that killed 32. The IS core was also able to send operatives to conduct attacks in Istanbul in June 2016 and January 2017.

However, the IS core has not been able to repeat that success in recent years. Today, the main terrorist threat posed by the IS network outside of the areas of operation of the core and franchise groups stems from grassroots jihadists, just as it does for al Qaeda. Because of this, it is important to take a deeper look at grassroots jihadists and the threat they pose.

Grassroots Jihadists

Al Qaeda's original operational model was to train individual operatives and then send them abroad to conduct attacks. Sometimes these operatives worked with local sympathizers to organize attacks—this was the model used in the 1993 World Trade Center bombing and the 1998 East Africa Embassy bombings. In the 9/11 attacks, the core sent a team to conduct the attack.

In the wake of 9/11, intense pressure was placed on the al Qaeda core. The core leadership became so frustrated by its inability to get operatives into the United States and Europe to conduct attacks that by 2009 it began to embrace and promote the leaderless resistance model of terrorism. Al Qaeda figures such as Adam Gadahn and Anwar al-Awlaki began to encourage al Qaeda supporters in the West to conduct simple attacks using readily available weapons near where they live, rather than attempt to travel to fight with the core and franchises or receive training from them. This resulted in increased attacks by grassroots jihadists such as the Little Rock,



Arkansas, shooting in June 2009 and the Fort Hood shooting in November 2009.

Encouraged by these attacks, al-Awlaki and his AQAP colleagues launched an English-language magazine in 2010 called *Inspire* that was intended to encourage jihadists living in the West to conduct attacks and provide them with rudimentary tutorials on how to conduct attacks. The bombmaking instructions in *Inspire* were used in several attacks, including the April 2013 Boston Marathon bombing.

Some grassroots jihadists are motivated and operationalized by a combination of al Qaeda and IS. It is not unusual to find grassroots jihadists who declare allegiance to the Islamic State but have watched sermons by Anwar al-Awlaki and read *Inspire* magazine. This makes grassroots terrorism somewhat nebulous. For example, in the January 2015 attacks in Paris, the brothers who attacked the offices of the satirical magazine *Charlie Hebdo* claimed allegiance to al Qaeda while their friend and co-conspirator who murdered a police officer and attacked a kosher grocery store claimed allegiance to the Islamic State.

Since the fall of the IS caliphate, a great deal of shine was taken off its appeal and its claim to be an inexorable force guided by divine power. Consequently, the number of IS-related grassroots jihadist terrorist attacks today outside of conflict zones is far lower than it was at the height of the Islamic State's power and prestige. Still, grassroots jihadists will continue to pose a persistent threat for the foreseeable future.

There are several common elements to both al Qaeda and IS-inspired grassroots attackers (note that these same characteristics also apply to white supremacists, anarchists, and others who practice leaderless resistance). First, they tend to operate alone or in small groups to help escape detection by law enforcement and security forces. This isolation comes with a price, however, and they tend to possess very little in the way of sophisticated terrorist tradecraft or official training from the core group or franchises. These factors mean grassroots attackers often struggle to plan and execute attacks. It also leaves operatives quite vulnerable to detection as they progress through their attack cycle, especially during surveillance and weapons acquisition.

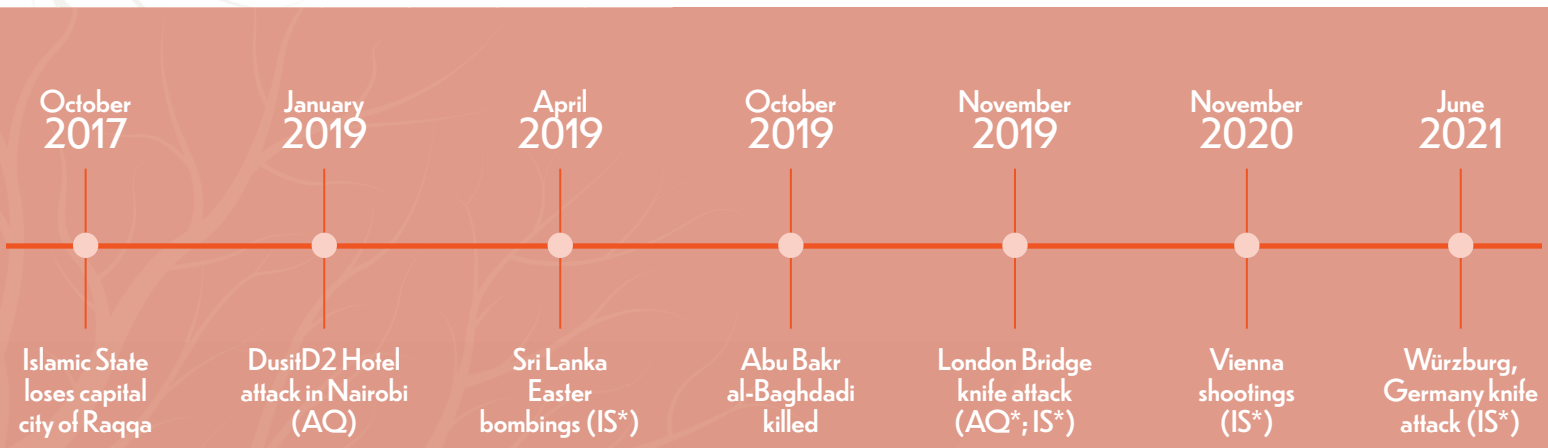
Many grassroots jihadists also lack the discipline required to be successful lone attackers and find themselves ensnared in government sting operations when they practice poor operational security by communicating with other extremists or reaching out for assistance with bombmaking or obtaining explosives and weapons. It is very rare that a lone attacker or small clandestine cell conducts a spectacular terrorist attack, regardless of the ideology.

> The frequency of jihadist terrorist attacks has been cyclical with discernable spikes and lulls.

The lack of terrorist tradecraft also makes it difficult for grassroots jihadists to attack hard targets, so they tend to focus their attacks on soft targets such as crowds of people on the street. This means that security measures can be implemented to harden facilities and deter would-be attackers.

There have been several examples of grassroots attackers who have been deterred from attacking a target due to the presence of video surveillance coverage and good access control. For example, a grassroots IS sympathizer who was arrested in Pittsburgh in 2019 and charged with plotting an attack on a church told an informant that he decided to attack the church rather than a Shiite mosque because the mosque locked its doors during services and had a video surveillance system. The IS sympathizer who attacked the Pulse Nightclub in Orlando in 2016 also passed up several potential targets he deemed as being too secure.

This is not to diminish the threat posed by grassroots jihadists; they do pose a very real and persistent threat and can be deadly. However, that threat is generally limited, and because of this, it is



more accurate to say that grassroots jihadists pose the most likely threat in the West, but not as severe a threat as one posed by people possessing sophisticated terrorist tradecraft.

Implications for Security Practitioners

Jihadism is a phenomenon that is intrinsically both global and local, and the nature of the threat posed by jihadists varies depending on location. This makes jihadist terrorism an ongoing and dynamic challenge for security practitioners, especially those managing multinational footprints. First, for those with interests in the countries where jihadist insurgencies are raging, the threat is significant. These jihadists seek to overthrow governments and establish jihadist polities. They will seek to create instability and ultimately a vacuum of authority so they can step in and establish control. To achieve this, they will not only attack security forces and other government targets, but also any other entity they believe to be supporting the government or promoting stability. Jihadists in various theaters have attacked aid and development workers, as well as commercial targets such at hotels, restaurants, tourist sites, and energy and mining concerns.

With the jihadist core and franchise groups strapped for resources, they will also be seeking to raise money and acquire resources. This means that they are likely to continue to conduct kidnappings for ransom, extortion, cargo theft, and raids to acquire food, fuel, weapons, and other materials. Many of these insurgents are highly mobile and able to cover vast expanses of land or sea—for example in the Sahel region of Africa and the Sulu Archipelago in Asia—so the reach of these groups can extend beyond their core areas. Additionally, some groups are known to work with regional criminal gangs, who will help with smuggling or even sell captives to jihadist groups.

Organizations with interests in regions surrounding core jihadist areas can expect insurgencies to continue their efforts to lash out against regional enemies and western interests.

The frequency of jihadist terrorist attacks has been cyclical with discernable spikes and lulls. Key events have a large influence on the tempo of attacks, and there have been spikes in activity following events such as the 9/11 attacks, the publication of cartoons featuring the Prophet Mohammed, and the IS declaration of a caliphate. It is likely that the world will experience periods of increased jihadist activity in the future, and it will therefore be important to watch for events that resonate among the jihadist rank and file and that can serve as triggers for attacks.

The threat of jihadist terrorism outside of the main theaters of jihadist insurgency will persist for the foreseeable future, but the danger it poses will remain limited so long as jihadist core and franchise groups are kept from becoming strong enough and secure enough to devote significant resources once again toward projecting terrorist power abroad. ■

Scott Stewart is the vice president of intelligence at TorchStone Global. He was the lead diplomatic security service special agent assigned to the 1993 World Trade Center bombing investigation and has investigated and analyzed jihadist terrorist attacks and activity since 1990.

Bridging the GA

Illustration by *Security Management*; iStock

Legal/Ethical

AP

Shifting regulation and decreasing consumer tolerance for corporate abuses of human rights may soon have non-compliant companies seeing both profits fall and losses in courtrooms unless they instigate a paradigm shift.

By Eva Nolle, CPP

THE RIGHTS TO LIFE, FOOD, EDUCATION, WORK, HEALTH, AND LIBERTY represent a range of fundamental and universal rights, inherent to everyone simply because of their inclusion in the human race. These rights are indivisible and interdependent—one right cannot be fully enjoyed without the others.

The United Nations (UN) adopted the Universal Declaration of Human Rights in 1948—the first legal document to address fundamental rights, with articles providing the principles of subsequent legislation, conventions, and agreements.

Because only countries can be party to international treaties, governments are responsible for enforcing, promoting, and protecting these rights. This, however, does not mean that private actors or entities, especially businesses, cannot impact human rights—either positively or negatively. In some instances, companies may even have a greater effect on such rights compared to governments.

The UN and other international organizations actively encourage corporate responsibility. But in the absence of law, human rights frameworks are currently not compliance issues and are often placed at the bottom of the corporate priority list.

Human rights issues are predominantly regarded as an ethical dilemma for companies, one that often triggers a "cost vs. ethics" debate to decide the course and extent of a response.

However, governing bodies—including the U.S. government, the European Union, and others—are increasingly passing legislation, such as Germany's Act on Corporate Due Diligence in Supply Chains (Lieferkettengesetz), that not only require businesses to respect human rights, but also conduct human rights due diligence (HRDD). HRDD detects and monitors operations' adverse effects on human rights, offering analysis into the impacts of upcoming legislative changes and how future issues can be avoided.

By their very nature, human rights abuses are an emotional topic. Even allegations of such incidents against a company will impact its reputation, and it will be on the company to allay the charges.

More Than Compliance

Human rights law is a complex speciality, and with an increasing focus on the intersection of human rights and businesses, it is not going to get simpler. Corporate departments outside of compliance and legal—especially professionals tasked with security and asset protection—will have to familiarize themselves with the changes.

A company can be held legally responsible not only for its own actions but also for incidents linked to its value chains, business relationships, or third-party contractors—even if it has not directly contributed to those impacts.

For a corporation, especially a large one, abuses will typically occur at the bottom of its corporate value chain, making them more difficult to uncover. Security professionals can help identify those abuses by piggybacking on existing frameworks and programs that already have due diligence procedures in place, rather than duplicating efforts.

The Cost of Human Rights

When seeking justice for human rights abuses committed by corporations, plaintiffs are largely dependent upon domestic criminal laws. Currently, most businesses accused of human rights violations enjoy impunity in the courts. The international community is inching toward converging existing non-binding regulations with binding laws. Consumers are becoming increasingly sensitive and conscious of how their buying power can reflect a spectrum of concerns—including ethics, corporate social responsibility (CSR), and environmental impacts.

With this heightened consumer and stakeholder scrutiny, corporate citizenship and conduct are becoming even more critical; companies need to consider how these matters impact their reputations and bottom lines. There are already more than a few initiatives dedicated to either exposing or ranking companies based on their sustainability and impact on people and animals, including the Clean Clothes Campaign, Good on You, and the Sustainable Brand Index. While most of these efforts focus on environmental issues, human rights abuses are garnering increased interest and creating a growing risk for corporations.

By performing a risk assessment, security professionals can assist other corporate departments to make an informed decision on how to treat the risks. And as always, prevention is better than a cure. Not only is prevention usually easier to manage, but it will most likely also be more cost-effective.

Security professionals need to monetize proposed solutions and programs, convert them into economic terms, and show a return on investment. But what is the price tag of human rights and how quantifiable are their negative infringements?

Human rights transgressions can negatively impact all corporate assets, including property, people, and information. Retaliation against abuses can take many forms—contaminated products, facilities attacked or vandalized, staff threatened or harmed, and much more.

But companies can also be targeted in the courtroom. Although legal remedies against non-state actors charged with human rights abuses are limited, companies can face criminal charges, and there are some precedents that lend themselves to be used as benchmarks for financial analyses.

In December 2019, a lawsuit was filed in the U.S. District Court for the District of Columbia on behalf of 16 children and their guardians from the Democratic Republic of the Congo (DRC). The defendants—Apple; Dell; Google's parent company, Alphabet; and Tesla—are accused of aiding and abetting in the deaths and serious injuries of children working in cobalt mines, which were part of the companies' supply chain for lithium-ion batteries. (*Doe 1 et al v. APPLE INC. et*

al, U.S. District Court for the District of Columbia, No. 1:19-cv-03737-CJN, 2019)

"This case is one of the first of its kind in the United States," says Terrence Collingsworth, attorney for the plaintiffs and executive director of International Rights Advocates. "It will set precedent, and there might be a whole lot more suits like this in the future."

According to the complaint, the companies knew about the unsafe mining practices due to public reports published by Amnesty International and others. Nevertheless, they allegedly failed to act and instead chose to exploit the system. Although all the defendants mentioned that their respective policies listed child labor as unacceptable, the suit claimed that no due diligence was conducted even though the cobalt industry is known for human rights abuses.

"The case could be settled, or it could go into a jury trial," Collingsworth adds. "A settlement would spare the defendants the discovery process and me and the world (from) seeing what is actually happening in their supply chain."

The plaintiffs have sued the five defendants and others for monetary, consequential, punitive, and exemplary damages, as well as "any and all other damages allowed by law according to proof to be determined at time of trial in this matter," according to the lawsuit.

"Any company takes a risk with a potential damage award of a U.S. jury," Collingsworth says. "It is hard to predict what a jury would look at, as many factors are at play, but it could be anything from $1 million upwards per life lost and even more for those victims that have been maimed for life."

In July 2020, 85 plaintiffs sought damages for assault and battery, rape, false imprisonment, and other serious mistreatment of employees at the hands of security guards employed by Kakuzi PLC, a major producer of avocados in Kenya. The lawsuit roped in Kakuzi's parent company, UK-based Camellia PLC, which is accused of negligence.

According to the suit, Camellia had a duty of care obligation because of its responsibility for Kakuzi's operations and its intervention, advisement, and supervision of relevant operations, including compliance with applicable corporate social responsibility standards. (*AAA & Others v. Camellia PLC et al.*, High Court of Justice Queen's Bench Division, No. QB-2019-002329, 2021)

In February 2021, Camellia agreed to a $6.4 million settlement, which includes payments to the claimants, a contribution to their legal fees, an independent human rights impact assessment, and investments in community projects.

To date, the company has spent more than $10 million on the settlement and related suits—including a $3.1 million settlement for claims against another subsidiary, Eastern Produce Malawi—and that figure is likely to rise.

Lydia de Leeuw from the Dutch Centre for Research on Multinational Corporations (SOMO), which was actively involved in the case, says the settlement is not the only impact on the company.

"Once the court case was filed and the human rights violations on Kakuzi's plantation became frontpage news in the *Sunday Times*, three UK supermarkets ended their collaboration with Camellia and publicly announced they'd suspend their purchasing of Kakuzi avocados, citing the human rights situation," de Leeuw says. "Not being able to sell these in the UK supermarkets will have a financial, as well as reputational, impact.

"Going forward, we will obviously monitor whether the company implements an effective grievance mechanism and human rights defenders' policy, as promised," de Leeuw says. "For this purpose, we also look at the supermarkets who should, rather than 'cut and run,' use their leverage to ensure that further human rights violations are prevented and past violations are remedied."

However, precedent is still nebulous in many cases and jurisdictions. In June 2021, the U.S. Supreme Court threw out a lawsuit against food corporations Nestlé USA and Cargill. The plaintiffs—six African men—accused the food firms of child slavery on farms in Africa, where they were forced to work on cocoa farms when they were younger. The plaintiffs said they were trafficked from Mali to farms in Côte d'Ivoire, working up to 14 hours every day, held captive by armed guards, and paid little besides the meals they ate. The men alleged that while the companies did not own or run the farms, they did buy cocoa from those farms and provided the sites with resources in exchange for exclusive purchasing rights.

In an 8-1 ruling, the judges dismissed the case because the human rights violations took place outside of the United States. The judges did not decide on whether U.S. companies were subject to the Alien Tort Statute, which allows non-U.S. citizens to pursue cases against U.S. citizens responsible for violations of international laws.

Emphasizing the current ambiguity, Justice Clarence Thomas wrote in the majority opinion that the courts needed to abstain from establishing a precedent where plaintiffs could successfully sue the companies. "That job belongs to Congress, not the Federal Judiciary. …Aliens harmed by a violation of international law must rely on legislative and executive remedies, not judicial remedies, unless provided with an independent cause of action." (*Nestlé USA, Inc. v. Doe et al.*, U.S. Supreme Court, No. 19-416, 2021)

The Void Between Legal and Ethical

As part of its corporate citizenship, a company is not only responsible for meeting legal standards, but also ethical ones. However, bridging the gap between these two demands can be frustrated by efforts to satisfy customers versus investing in corporate social responsibility. Some customers want their products as cheap as possible, without consideration for the global consequences, while other consumers are increasingly aware of human rights issues.

Operating within economic and price pressures while being ethical is possibly one of the biggest conundrums for businesses to conquer in the 21st century. The fact that there are currently few laws or regulations stipulating that companies have to respect human rights only increases the dissonance.

Operating within economic and **price pressures while being ethical** is possibly one of the biggest **conundrums for businesses** to conquer in the 21st century.

However, companies operating in high-risk areas and industries recognized a while ago that profitability and human rights are not necessarily mutually exclusive. In fact, CSR can help companies operate more effectively.

The Voluntary Principles Initiative (VPI) is a multi-stakeholder initiative established by extractive industry companies, non-governmental organizations (NGOs), and the governments of The Netherlands, Norway, the United Kingdom, and the United States. Today, the initiative also includes observers and companies involved in harvesting, developing natural resources, and energy.

The VPI promotes implementing a set of standards that guides companies in conducting a comprehensive human rights risk assessment in their engagement with public and private security providers, which ensure human rights are respected. Together, members share information that strengthens their capacity to address complex security and human rights issues in business operations around the world.

The initiative provides companies with guidance and tools to understand the environment corporations operate in, identify security-related human rights risks, and take steps to address them. It helps companies anticipate likely situations in which human rights abuses occur and develop on-the-ground strategies to mitigate them.

As the signees of the principles predominantly operate in challenging operating environments, they adopt the framework to not only minimize the risk of litigation and reputational damage, but also to maintain their social license to operate, foster investor confidence, and reduce operational and security risks.

While the above initiative is a collaboration between NGOs, companies, and governments, other initiatives have been established by international organizations and recommend measures for businesses.

The Organisation for Economic Cooperation and Development (OECD) published its *Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas* for the first time in 1976 and has since occasionally updated it. As minerals frequently come from conflict-affected areas where good ethical governance is not applied, the potential for human rights abuses to occur in these areas is relatively high. The framework provides recommendations for companies to respect human rights, as well as guidelines on using detailed due diligence as a basis for responsible security management.

In 2011, the UN published its *Guiding Principles on Business and Human Rights,* which laid the foundation for HRDD globally. The document outlines the duties of governments to protect human rights and corporations' responsibilities to respect such rights, as well as access to remedy any violations. They were written to apply to any business, regardless of its size, sector, location, ownership, or structure. While they do not claim to create a legal obligation, in the absence of applicable laws, the principles have become a standard for most businesses that wish to implement a framework. Additionally, many legal frameworks that have since been implemented or are being drafted use the *Guiding Principles* as their foundation.

The Legal Future

In 2014, the UN Human Rights Council set up an open-ended intergovernmental working group (IGWG) on transnational corporations and other business enterprises with respect to human rights. While the working group started slow, it gained significant ground in the last two years, publishing its second revised draft in late 2020 for a legally binding instrument that is supposed to regulate the activities of business with regards to international human rights laws. (A third draft is expected to be tabled by July 2021.) Although it will eventually become a treaty and thus only binding for countries, its purpose is to assist governments in implementing the necessary prerequisites. It also puts an obligation on governments to include a system of legal liability for human rights abuses that may arise from business activities—both from natural and legal persons—in their domestic laws.

While anti-corruption programs predominantly operate under **a perpetrator-centric perspective,** the focus of a human rights program **would be primarily victim-centric.**

Some countries have already implemented applicable legislation and other jurisdictions are rapidly following suit, with legal requirements becoming increasingly specific.

The UK Modern Slavery Act 2015 makes provisions for slavery, forced human trafficking offenses, and protection of victims. It requires UK-based businesses with an annual global revenue of at least £36 million ($50 million) to publish an annual slavery and human trafficking statement disclosing what steps have been taken to ensure such incidents do not occur in their supply chain.

The 2017 French Loi de Vigilance mandates that large French companies publish and implement a plan to identify and prevent human rights risks linked to their activities.

The Australia Modern Slavery Act 2018 requires entities that are based or operating in Australia—with an annual consolidated revenue more than A$100 million ($73.4 million)—to report on the risks of modern slavery in their operations and supply chains, as well as how they addressed those risks.

In July 2019, the U.S. House of Representatives introduced an amendment to the Securities Exchange Act of 1934—the Corporate Human Rights Risk Assessment, Prevention, and Mitigation Act of 2019 (CHRRA Act). Although this bill failed to pass prior to the end of the House's term, it may be reintroduced in the future, and other bills are being discussed in the U.S. Congress that could effectively prevent the importation of products made with forced labor and other extreme human rights violations.

In June 2021, the German parliament adopted the Lieferkettengesetz, which will require companies to regularly identify, mitigate, and prevent risks associated with their own activities and those of their subsidiaries, suppliers, and subcontractors. The law is scheduled to come into effect in 2023. It first requires larger companies to conduct the checks, extending its scope to smaller businesses in 2024.

Austria, Denmark, Finland, Luxembourg, and The Netherlands are working on legislation that would enforce HRDD enquiries for a company's supply chain, and the European Commission has committed itself to tabling an EU-wide HRDD law in 2021.

The Road Ahead

The sheer volume of legislation being drafted or already implemented will mean that most companies will probably have to adhere to a human rights law within the next few years. Even if a business is based in a jurisdiction that does not require HRDD, it may be beneficial for it to start proactively identifying risks and establishing a relevant framework.

It is also clear that companies, especially those with an abundance of suppliers, cannot exercise complete oversight over the entire supply chain on a continuous basis. Therefore, HRDD lends itself to a risk-based approach, particularly when first implementing the framework and vetting companies that are part of the supply chain.

Companies can begin by assessing their supply chain based on jurisdictions or industries and assigning risk profiles to them—ultimately identifying which parts of the supply chain are highly vulnerable to human rights abuses and should be examined first. High-risk areas for human rights abuses are characterized by a country's inability or unwillingness to fulfil its own human rights obligations, along with political instability or repression, institutional weakness, insecurity, collapse of civil infrastructure, and widespread violence.

Corruption thrives in similar environments and can pose a separate risk while impeding a company's ability to access necessary information. Like anti-corruption programs, achieving compliance with HRDD frameworks will rely heavily on conducting due diligence inquiries within the supply chain. Therefore, security professionals can use existing programs with a slightly changed approach. While anti-corruption programs predominantly operate under a perpetrator-centric perspective, the focus of a human rights program would be primarily victim-centric. Modified accordingly, they can accommodate for the identification, analysis, and treatment of actual and perceived human rights abuses, as well as other adverse social responsibility impacts.

An HRDD framework will certainly depend on company size, type, legal structure, geographical area, and industry, as well as other laws and regulations it operates under. Nevertheless, most HRDD legislation will likely align with the UN *Guiding Principles*. In the absence of legal requirements, they can be used as a guideline to set up the framework.

Equally, ISO 26000:2010, *Guidance on Social Responsibility*, promotes responsible practices in organizations while considering a variety of social responsibility issues, including human rights. It has a similar approach to the OECD Guidelines in that ISO 26000 provides guidance rather than requirements and cannot be certified like other ISO standards.

By aligning its policies to any of the three above existing guidelines and adhering to it, a company will have already taken major steps and positioned itself well for the inevitable regulatory shifts. ■

Eva Nolle, CPP, CFE (Certified Fraud Examiner), specializes in commercial intelligence, including due diligence enquiries, background screenings, political risk analysis, and commercial and fraud investigations. During the last decade, she has assisted clients operating on the African continent to gain a better understanding of potential risks when operating on the continent and how to avoid, mitigate, transfer, accept, or exploit them. Nolle holds a bachelor's degree in risk and security management.

Global Management

How Security is Changing in Latin America

Organized crime, shifting workforces, and stricter hiring requirements are influencing the role of security leaders across Latin America.

Security management is a global profession. Every region of the world has threats that need mitigation; every organization has people and assets that need protection. But the practice of the profession is also influenced by local conditions—culture, business practices, economics, politics, and type and severity of threats—that differ from region to region.

With that in mind, this ongoing Global Management series from *Security Management* highlights security managers from different regions of the world to learn about the challenges they face and the management strategies that help them succeed.

In this installment, we turn to Latin America. While each region, country, and state have unique challenges and cultures, security professionals are facing broad risks from evolving criminal activity and subsequent economic instability. Changing elements in the workplace—from certification-focused hiring managers, a younger workforce demanding respect and inclusion, and the influence of digital transformation—have driven security professionals to build robust local networks and pursue more proactive business and security strategies.

These conversations have been lightly edited for length and clarity.

Illustration by *Security Management*

Lourdes Morales Aguilar *is prevention tribe lead for Walmart Mexico and Central America. A Costa Rican criminologist with more than 16 years of experience in the security field, she is responsible for corporate security, emergency management and response, executive protection, investigations, security operations, and supply chain security. Aguilar describes herself as a disruptive, adaptable, and curious security professional, which enables her to challenge cyclical security processes and develop tailored security solutions.*

What are a few of the common challenges that a security manager may face working in Mexico?

LA. Crime and resulting insecurity are some of the most serious problems that Mexico has faced in recent decades. According to the *National Victimization Survey 2020 (ENVIPE)*, during 2019, 29.2 percent of the country's homes had at least one crime victim. The same survey indicated that in 2019 there were 30.3 million crimes associated with 22.3 million victims in the country, which represents a rate of 24,849 victims per 100,000 residents during that period.

ENVIPE pointed out that 68.2 percent of the population over 18 years of age said public insecurity is the main problem afflicting Mexico, followed by unemployment (34.6 percent), and health (with 36.2 percent). Similarly, 78.6 percent of the population said that living in their state is unsafe because of crime.

Speaking about crime, unemployment and poverty always emerge as determining factors. In turn, crime also causes greater poverty—creating a vicious circle that is difficult to break.

In just one year, the impact of the coronavirus pandemic on the Mexican economy has been catastrophic. The gross domestic product (GDP) had its worst fall in almost a century, plummeting 8.5 percent in 2020, which in turn caused thousands of Mexicans to lose their jobs. Mexican economists estimate that the pandemic will cause nearly 12 million people to fall into poverty, which would affect almost 26 percent of the population.

In your view, is the relationship between manager and employee changing in Latin America? How does workplace culture today compare with years past?

LA. The introduction of flexible ways of working has taken a significant leap during the COVID-19 pandemic. Companies have accelerated their digitalization processes at full throttle to adapt, first to confinement measures and now to design what the new environments will be like.

In recent months, companies have been able to verify that teleworking has favored work for objectives over work for dedicated hours, that employees greatly value this flexibility, and that technology can support the demand for remote connection, allowing practically all types of operations. Everything indicates that teleworking and labor flexibility will be the levers of the new labor reality.

Also, many companies have realized that maintaining sustainable business performance requires the ability to attract and retain a diverse workforce.

Diversity and inclusion mean that all individuals have equal opportunities, regardless of their ethnic group, country of origin, sexual orientation, race, ability, gender, age, or even personal interests. It is not just about job opportunities—it is about people feeling safe as who they are, and that their different experiences, values, and perspectives are appreciated, rather than something that could harm them.

Given your experience as a business leader, do you see the role of the security department changing with some Mexican or Costa Rican companies?

LA. Risks, threats, and crises have become more complex and sophisticated; with this came the need to anticipate them through the application of preventive measures and the use of data. But this does not exempt companies with a greater size, complexity, or geographic presence from continuing to face crisis situations that require an immediate response.

In crisis management, the speed of response is essential—driving an accurate diagnosis of the threat and the implementation of an immediate action plan with the necessary resources to carry it out. And both the diagnosis and the action plan must be comprehensive and deal with all those aspects—operational, communication, legal, technological, or financial—that allow a rapid recovery of the company's situation.

Prevention and reaction must be in perfect balance to guarantee the success of security teams.

Servio Camey, CPP, *is regional security manager for Central America and the Caribbean for Bayer. He is responsible for physical security, strategic security, intelligence for early risk or threat detection, brand protection, managing anticounterfeit or contraband investigations in the region, logistics security, and ensuring the quality of products and a safe working environment for employees. Camey is based in Guatemala.*

What are a few of the common challenges that a security manager may face working in Central America?

SC. Central America has to be divided in two areas—one is from Nicaragua to Panama, and the other is the northern triangle of Guatemala, El Salvador, and Honduras. This is the biggest challenge of all because these countries are the birthplace of gangs and extortion, and any security manager in the region has to be very well versed in handling extortion, kidnap, and negotiations. Constant training, preventive security, and risk analysis are essential when working in countries that are in the top 20 most

violent countries in the world. But I have learned that due diligence in all we do will keep you with zero incidents if you have a consolidated team that has good cohesion, global policies, and local procedures in place.

Another challenge is social disruptions; the region is volatile in social activity. We have seen Nicaraguans block roads for 20 days in which all raw materials or products have been halted—nothing could pass either way, and millions of perishables were lost. Honduras has also seen social violence. In one incident, a banana company lost more than 20 containers burned down by protesters in one day. Costa Rica has blocked its border with Panama due to feuds with trucker unions, so having good intelligence, crisis management, and business continuity plans is vital in the region.

And last, corruption is present mostly from Guatemala to Nicaragua and in way lesser quantity in Costa Rica and Panama. A good security manager in the region has a compendium of laws for the six countries, as well as contacts to tend to logistic emergency response in case of accidents or loss in transit. Managing a region as complex as Central America tests your skills and brings the best out in every security department—the key to win is the application of best practices and standards in your operation.

How has organized crime in Latin America affected your role as a security professional? Has that changed in recent years?

SC. Definitely; organized crime has evolved greatly, not only in the traditional ways but now has online services, social engineering, cryptocurrency to hide its money, hostile takeovers of legitimate businesses, and transnational structures like MS-13 working with Mexican cartels from El Salvador to the United States. This is something we have to observe closely, so keeping our sources of information, intelligence units, and contacts with local law enforcement up to date is vital. Also having a good relationship with your local Overseas Security Advisory Council (OSAC, part of the U.S. State Department) chapter is highly recommended.

Organized crime infiltrates cargo areas in ports, so even if you are Customs-Trade Partnership Against Terrorism (CTPAT) or Authorized Economic Operator (AEO) certified, we have seen containers get contaminated at ports. That is an influence of organized crime that is out of your hands, and you have to be observant and ready to manage such issues. Good risk management and due diligence will go so far, but there will always be things that go beyond our control.

If I am a security manager for an international firm being transferred to a Central American office, what advice would you give me?

SC. In my experience, the power of networking will do wonders for the modern security manager; you can contact a peer in any country, and he or she will give you an objective analysis on the cultural issues, political background, social structures, and common risks. Don't ever rely on a document or assessment from someone who does not live in the country you want the information from—those documents are usually put together by think-tanks interested in giving you services to counter the risks that they themselves are telling you exist. Associations, groups, and chats all have their merit, but remember—no document you read is good without local testimony to verify the information.

In your view, is the relationship between manager and employee changing in Latin America? How does workplace culture today compare with years past?

SC. It's the million-dollar question. In Latin America, security in the past was forced through fear and intimidation, limited to physical security with no knowledge whatsoever of policies or procedures, and security departments didn't have respect and trust as their standard. People with former military backgrounds had all the security positions, and their word was law.

Now companies are migrating to a prepared professional that knows how to enforce security and understands the process of identifying risks and the strategies to mitigate these risks.

How has the COVID-19 pandemic changed leadership regionally and for you specifically? How did it change the role of the security department?

SC. COVID-19 gave security the visibility of a lifetime. Local security at companies had to cross functions with health, safety, and environment (HSE) to form the first line of defense and protect our employees from COVID-19. Guards went through intensive trainings of preventive measures that not only helped the company but also employees and their families.

The pandemic gave us a new opportunity to show security's capabilities and adaptability. As security managers, we were used to providing a daily presence and supervision, but all of a sudden we found that security in the region had a very large technological gap. Guards found themselves using Zoom, Skype, and other platforms that they did not know due to low scholarship. But now, it's all part of the new normal in security.

COVID-19 changed many things; it has given us the opportunity to evolve and keep growing, learning, and adapting. This is what we do to keep our people safe.

Paulo Grechi de Almeida, Sr., CPP, PCI, PSP, *is security manager in Brazil for global financial services technology firm Fiserv, where he is responsible for managing the in-country corporate security program, providing a safe and secure work environment for personnel while protecting company and client assets. Almeida is based in São Paulo, Brazil.*

What is it about your life experience, your personality, and your background that helps make you an effective security manager?

PA. Having been a Brazilian Army officer helped me in my sense of mission accomplishment and leadership styles, which are essential for success in the private sector as well.

Having gone through several positions in the private security in-

dustry—from the junior to senior level, performing different types of tasks, and working in different industries—gave me a more complete understanding of the security industry practical experience.

Having an MBA, a postgraduate degree in administration, and a degree in private security also contributed to the knowledge that is required on a day-to-day basis, such as project and contract management, performance evaluations, budgeting, and sector-applicable legislation, among others.

Managing a region as complex as Central America tests your skills and brings the best out in every security department.

The fact that I have had contact with technology and games since I was a kid also contributed to making my daily tasks easier when using technology tools and adapting to new technology solutions that appear every year.

What are a few of the common challenges that a security manager may face working in Brazil?

PA. The challenges are evolving all the time here in Brazil, but we still have a certain difficulty in accessing the most modern security solutions and systems and importing them at an affordable investment. The Brazilian currency is devaluated against other currencies. I think we need to further strengthen our domestic industry.

Another difficulty is the limited number of service providers and specialized labor capable of covering the entire national territory, which is huge (Brazil covers more than 3.2 million square miles). This sometimes impacts the quality of service level agreements, such as security system maintenance response times.

In Brazil, it is becoming more common for companies to have administrative offices in commercial buildings with shared spaces. The interdependence between internal real estate, facilities, IT teams, and condominium access controls and security infrastructure may pose challenges to the corporate security managers' ability to manage local risks and implement physical security and other protective measures.

Therefore, it is extremely important to have well defined roles and responsibilities for each party, foster an excellent relationship, embrace flexibility, and promote the ability to create innovative solutions—always thinking about cost vs. benefit while reducing risks.

Has the political climate in Brazil affected your work as a security professional?

PA. Unfortunately, the political climate in Brazil has been unstable for some years, but now with the current scenario of COVID-19 and its health and economic consequences to the country, it has caused the entire society—including security professionals—to need a much higher level of resilience and constant adaptation. In terms of work, it increased the dependence on security systems with remote management capacity and less physical presence, and it increased the importance of media monitoring, geopolitical analysis, and travel security programs.

If I am a security manager for an international firm being transferred to the São Paulo office, what advice would you give me about how I can avoid making mistakes when it comes to cultural issues that influence employee relations and the workplace?

PA. I believe that mastery of a basic level of Portuguese is essential for the professional to understand the daily issues of the work environment and communicate. Foreign languages such as English and Spanish are still a local barrier; a low percentage of the population speaks a foreign language, and local services in general are not yet fully adapted to receive foreigners speaking other languages.

Some states are larger than countries, so we have different cultures within Brazil that affect the way people relate, speak, and act. The modus operandi of crimes, crime types or rates, and the structure of organized crime can vary by region. Therefore, contacting local security specialists who know the area is fundamental and will help in the correct assessment of criminal risks and rates.

Another suggestion is to have good legal support and some knowledge of local laws that affect the security industry—such as the new privacy law the General Personal Data Protection Act (LGPD)—and the specific laws and ordinances of the Federal Police, because private security activities in Brazil are regulated, authorized, and supervised by the Federal Police Department.

Do you see the role of the security department changing with some Brazilian companies?

PA. Yes, the security department is increasingly being involved, listened to, and called to help businesses units make decisions at a strategic level, for example on issues involving the opening or closing of sites, retrofits, and mergers and acquisitions in other regions of Latin America.

Security and safety policies, standards, guidelines, and indicators from security systems, risk assessments, compliance requirements, and incident reports have become fundamental factors to assist decision-making executives. For this reason, standardization, quality, and confidence in the information gathered are essentials to be presented at the executive level. ■

Claire Meyer is managing editor for *Security Management*. Connect with her on LinkedIn or via email at *claire.meyer@asisonline.org*.

SECURITY TECHNOLOGY

THE STRAIN OF CLIMATE CHANGE

// *By Megan Gates*

In a year of unusual activity, an unusual phenomenon stood out: in April 2020, carbon dioxide emissions dropped by almost 2 billion tons to their lowest point since World War II, according to the International Energy Agency (IEA).

Environmentalists hailed the moment, urging nations to commit to further reducing emissions to limit the impact of climate change. But it was short lived. In December 2020, the IEA said the resurgence in economic activity due to pandemic recovery measures was pushing energy demands higher than pre-COVID-19 levels.

And this could pose major ramifications for global security, which is already feeling the strain of emissions-induced climate change in the form of major weather events, migration, and drought. For the second year in a row, environmental experts and security practitioners raised the alarm on this threat in *The World Climate and Security Report 2021*—published by the International Military Council on Climate and Security (IMCCS).

The report warns of the compounding security threats posed by the convergence of climate change and other global risks, like COVID-19, and the strain they will place on critical infrastructure and security personnel around the world.

"Major and urgent global emissions reductions are necessary in order to avoid significant, severe, or catastrophic global security consequences in the future," said IMCCS Secretary General Sherri Goodman, former U.S. deputy undersecretary of defense. "We also need to climate-proof all elements of security—including infrastructure, institutions, and policies....The transition from concepts of climate security to implementation is critical and urgently needed." ■

To continue reading this article and more of the August 2021 issue, visit *asisonline.org/SecurityTechnology*

Photo by iStock

SECURITY TECHNOLOGY

Read these articles and more online at
asisonline.org/SecurityTechnology

Protecting the Bulk Power System a Connection at a Time

UTILITIES SECURITY

By Ross Johnson, CPP

The North American power grid, dubbed the Bulk Power System, is a network of networks that encompasses power generation, transmission to communities, and distribution to commercial and residential customers.

The day-to-day work of protecting the grid starts with the asset owners and operators. In cyberspace, state-sponsored actors and criminal hackers attack the grid millions of times per year. Monitoring, preventing, and responding to this onslaught is an around-the-clock responsibility. In the physical world, the distribution networks in communities are often targeted by thieves, looking for copper to sell to recyclers, or tools and equipment. Prevention requires the full range of physical security skills.

An Energy Company's Proactive Approach to Security

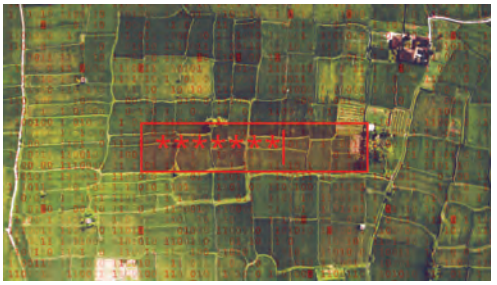
OPERATIONAL TECHNOLOGY

By Brian Romansky

Given today's increased threat level to operational technology, a large North American energy company decided to proactively use data diodes as a critical component of its defense-in-depth strategy.

The security architecture development was guided by a segmentation assessment to see what critical control systems could be modified to work in a one-way only mode, such as broadcasting data without expecting confirmation.

That model fits with U.S. Department of Homeland Security guidance to convert as many connections as possible to hardware one-way only paths, and then focus defenses on communication that must remain two-way.



The Next Target: Agriculture and the Supply Chain

AGRICULTURE SECURITY

By Greg Gatzke

The U.S. Department of Homeland Security named agriculture as one of the top areas of critical infrastructure that are at risk in today's threat landscape. Just a few months ago, a ransomware attack on JBS Foods, a food production company that is the world's largest processor of fresh beef and pork, targeted operations in Australia, Canada, and the United States. It caused 13 plants to close temporarily, significantly reducing supply.

Just like the Colonial Pipeline hack that caused operators to shut down the systems that supply 45 percent of fuel to the Eastern Seaboard, cyberattacks on the supply chain cause prices to soar, demand to increase, and supply to wane. And our food supply will continue to be a target.

A WATER CRISIS

Water is essential for life. But it also poses a great danger when there is too much or too little of it. A new assessment by the World Meteorological Organization found that of the 10 disasters that caused the most human fatalities in the past five decades, drought killed the most people. *The Atlas of Mortality and Economic Losses from Weather, Climate, and Water Extremes (1970-2019),* to be published in September 2021, found that:

650,000
deaths were caused by drought

577,000
deaths were caused by storms

58,000
deaths were caused by floods

Source: *The Atlas of Mortality and Economic Losses from Weather, Climate, and Water Extremes (1970-2019),* World Meteorological Organization, September 2021

Images by iStock

AIRPORT SECURITY

Singapore's Changi Airport Group selected Genetec, Inc., as a security solutions partner for the airport's three-year security expansion and upgrade project. With the system, the airport—which is one of the largest transportation hubs in Asia—plans to improve the overall experience for passengers, employees, and business operations. The project is expected to reach completion by the end of 2023, and it will integrate the civilian airport with Genetec Security Center, a unified security platform which combines IP security systems into a single interface, with a specific focus on terminals' video surveillance system. Security Center will allow airport security managers to accommodate for new data types within a single interface, underpinning the facility's security operations.

MERGERS & MOVES

Teledyne Technologies ⇆ FLIR Systems

The approximately $8.2 billion acquisition will rebrand the company as Teledyne FLIR, expanding Teledyne's portfolio with digital and thermal imaging solutions.

Deloitte & Touche LLP ⇆ CloudQuest, Inc

Deloitte's purchase will complement its cloud security orchestration, automation, and response services.

Elbit Systems Ltd. ⇆ BAE Systems Rokar International Ltd.

The acquisition of Rokar will enhance Elbit's ability to support high-end GPS receivers and guidance systems.

SFP Holding, Inc. ⇆ Reliable Fire Protection

Reliable Fire Protection and nine other companies will expand SFP Holding's presence into 18 U.S. states.

Award

Eventus Systems, Inc., won the Trade Surveillance Product of the Year award in the 2021 Risk Technology Awards. This is the second time the company's Validus platform has received this recognition.

Contract

Raft, LLC, was awarded a $36 million contract to provide the U.S. Air Force Life Cycle Management Center's AFLCMC Detachment 12, "Kessel Run," with DevSecOps expertise, specialized infrastructure, and other services.

Announcements

3xLOGIC, Inc., introduced its Gunshot Detection solution, which can be used as a self-contained device or integrated into existing systems to detect the concussive force produced by gunshots.

Partnerships

Utilities

Everbridge and Wiznucleus partnered to increase their digital and physical security offerings to some of the largest nuclear, electric, and other energy supply companies.

People Counting

SAFR from RealNetworks, Inc., partnered with Dains to launch a solution that increases the accuracy of people counting to prevent duplicates of customers and employees.

Networking

PSA added NETGEAR to its network, offering clients highly flexible and scalable network switches, as well as routers, extenders, wireless airbridges, and Wi-Fi range extenders.

Image courtesy of Genetec, Inc.

The Security Profession Reconvenes at GSX

By John A. Petruzzi, Jr., CPP, ASIS President 2021

Petruzzi speaks at GSX 2019 in Chicago, Illinois.

Global Security Exchange (GSX) is among my favorite traditions. Community and collaboration are the hallmarks of the security profession. We all share a goal of making the world a safer place, and we are all committed to helping each other reach that goal. As an ASIS member for more than two decades, I can confidently say that community and collaboration are the pillars that keep me coming back to ASIS International and to GSX.

GSX is the culmination of those values. It's where we come together with our peers to share information about tried and tested solutions for the problems we share as security professionals and hash out plans of attack for the threats looming beyond the horizon.

Between attending world-class education sessions, witnessing new vendor technologies on display, and forging connections with colleagues whose collective experience can help you tackle whatever issues you're currently going through, it's almost impossible to leave GSX without a new, better approach to the way you do business.

I will be among those who will meet—safely—in-person at the Orange County Convention Center in Orlando, Florida, from 27–29 September. However, if you aren't able to join us in-person, the GSX Digital platform provides a comprehensive virtual experience, wherever you are.

In the midst of a pandemic the likes of which none of us have ever seen before, it didn't feel right for vital GSX discussions to be restricted to only those who are willing and able to travel. From the time the platform kicks off on 15 September, the GSX Digital experience builds on the success of 2020's entirely digital Global Security Exchange Plus (GSX+) to deliver GSX content and training anywhere in the world.

What's more, if you miss the "live" GSX

20 Years Later: Remembering Those We Lost on 11 September 2001

In honor and memory of our colleagues in the security profession whose lives were lost in the performance of their duty on 11 September 2001 in New York, and all others who have been called upon to make the ultimate sacrifice, ASIS International values the courage and commitment of the following individuals:

- Patrick Adams
- Godwin Ajala
- Andrew J. Bailey
- Francisco Bourdier
- Larry Bowman
- Edward Calderon
- Mannie Leroy Clark
- Denny Conley
- James Corrigan
- Francisco Cruz, Sr.
- Titus Davidson
- Samuel Fields
- John R. Fisher
- Godwin Forde
- Ervin Gailliard
- Ronald G. Hoerner
- Lamar Hulse
- Mohammed Jawara
- Charles Gregory John
- Douglas G. Karpiloff, CPP
- Howard B. Kirschbaum
- Charles Laurencin
- Daniel Lugo
- Robert Martinez
- Stanley McCaskill
- Jorge Morron
- John P. O'Neill
- Alexander Ortiz
- Richard Rescorla, CPP
- Esmerlin Salcedo
- Nolbert Salomon
- Frances Joseph Trombino
- Jorge Velazquez

dates this 27–29 September, you can still unlock GSX education from the comfort of your home or office. By registering for GSX Digital after the event, you can participate in encore events we have scheduled for the remainder of 2021 and view recordings of the best education sessions your security peers can offer.

GSX helps keep the lights on at ASIS International, allowing us to continue providing you with the year-round community and collaboration you expect from ASIS. If you plan to take part in this year's show, our 34,000-member association thanks you for your support.

As the first in-person GSX in a little more than two years, this year's GSX means a little bit more for many of us. It serves as the first opportunity in that time for us to reconnect with many valued colleagues and friends. Whether in-person or digital, whether live or time-shifted, I hope you are able to join us and benefit from the ultimate professional development event our profession can offer.

You can learn more about this year's event at *GSX.org*. Thank you.

Access the Latest *Information Asset Protection Guideline*

As an American National Standards Institute (ANSI) accredited standards developing organization, ASIS International is a world leader in developing standards and guidelines to serve the needs of security practitioners in today's quickly changing environment. ASIS members are entitled to exclusive access of these premium security management resources, like the newly updated *Information Asset Protection (IAP) Guideline*.

The *IAP Guideline*, applicable to organizations of all sizes and types, specifies steps that an organization can take to develop and implement an effective risk-based information asset protection program. It provides guidance on program development and maintenance and outlines management, legal, and security strategies organizations can employ to safeguard their information assets.

Earlier in 2021, ASIS International published timely revisions to its *Physical Asset Protection Standard* and *Business Continuity Management Guideline*.

Other published standards and guidelines provide guidance on a wealth of security management topics, including:

- Risk assessment;
- Workplace violence and active shooter prevention and intervention;
- Supply chain risk management;
- Security awareness;
- Investigations;
- Enterprise security risk management (ESRM);
- Pre-employment background screening; and more.

ASIS members enjoy free e-book access for all ASIS standards and guidelines. Softcover versions are available for purchase at the ASIS Store.

In addition to its role developing standards, ASIS serves a key liaison role on two International Organization for Standardization (ISO) technical committees. Learn more at *asisonline.org/Standards*.

ASIS Celebrates Security's Best

Every year, ASIS recognizes the important work of ASIS members around the world with awards that celebrate their accomplishments and dedication to the security management profession. ASIS is honored to recognize the

ASIS Global Events

SEPTEMBER

15 GSX Preview Event - Digital

27–29 Global Security Exchange - Orlando, Florida, USA, and Digital

ASIS Education Webinars

SEPTEMBER

1 Advanced Concepts in Business Continuity & Crisis Management

OCTOBER

19 Cyber Incident Response: Common Pitfalls

26 Cybersecurity and Physical Security Convergence

View all educational offerings at *asisonline.org/education.*

following outstanding individuals for their accomplishments during the past year.

- **President's Award of Merit: Dana W. Adams, CPP, and Jaime P. Owens, CPP**
  Bestowed by the president of ASIS International to an individual member for distinguished service, achievement, and/or contributions. Distinguished achievement includes significant contributions to the knowledge of the profession, literature of the profession, outstanding service to ASIS International, and/or service to other organizations affiliated with the security profession.
- **Women in Security Global Community Karen Marquez Honors: Lynda L. Buel, CPP**
  Honors an ASIS International female security professional who has consistently worked for the betterment of the security industry.
- **Young Professional of the Year Award: Angela J. Osborne, CPP, PCI, PSP**
  Honors an ASIS International member under age 40 who demonstrates a dedication to the security industry through strong leadership, teamwork, and innovation, while continually developing their knowledge and experience, necessary in this ever-changing industry.
- **Ralph Day Memorial Security Officer Heroism Award: Jacqueline Green, Sunstates Security**
  Recognizes outstanding service or acts in the security profession. This award is meant for those who perform a heroic act that involves circumstances where a private security officer risks his or her life to save another person. It is bestowed by the ASIS Security Services Community (SSC).
- **E.J. Criscuoli, Jr., CPP, Volunteer Leadership Award: Ronald Lee Martin, CPP**
  Celebrates an ASIS International member who has exhibited selfless devotion at the

#MYASIS IMAGE OF THE MONTH

ASIS WIS Kenya Chapter

We are excited to kick-off the ASIS - Kenya chapter Security Week today.... As the number of women in the industry grows and women look to support and help each other in the various disciplines and practices of security, ASIS Women In Security Kenya formed to achieve that common goal. #MyASIS

ASIS CERTIFICATION PROFILE // PAMELA MISCHO, CPP

Pamela Mischo is persistent. She gets the job done. She began her security career in high school—working retail security at her local department store. She has stuck with the career ever since.

"What I liked about the job was the chase," she says. "The adrenaline and satisfaction of a job well done by preventing loss to the store meant something to me."

After a few years, she moved into management at the store, where she had the opportunity to expand her skill set to include internal investigations and supervisor duties. After about 10 years working for the retailer, with an

associate's degree in criminal justice/police science under her belt, she had the opportunity to move into a corporate security position.

Now, armed with a bachelor's degree in criminal justice and pursuing a master's degree in crisis, emergency, and disaster management, Mischo serves as manager of global security – Americas, for a major pharmaceutical corporation. She oversees 16 sites throughout the United States, serving as their global security point of contact.

She joined ASIS International in 2010, when her organization's entire global security team was encouraged to join. She became involved because she wanted to achieve the Certified Protection Professional (CPP®) designation—and the benefits that accompanied it.

With that destination in mind, she achieved her goal in 2019. "The accomplishment that I felt when I received my score report with that bright green circle that said 'PASS' reinforced that I'm qualified to be where I am," she shares. "I earned it—and will do everything in my power to retain it! The CPP exam was the hardest thing I have ever had to study for."

Mischo's persistence was key in achieving her CPP, and she suggests that others who follow in her footsteps remain dedicated to the task.

"Study, study, and study some more," she recommends. "The universal recognition that you receive for being a CPP is worth all the effort that it takes to earn it."

Profile by **Steven Barnett**, ASIS Communications Specialist

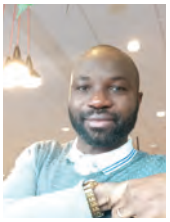
volunteer level, emphasizing significant contributions at the chapter and regional levels over an extended period of time.

- **Don Walker CSO Center Security Executive Award: Joe Olivarez**
  Recognizes a senior-level executive who demonstrates commitment to security management education, certification, and standards and guidelines for the executive management level of the security discipline in a given enterprise.
- **Roy N. Bordes, CPP, Community Member Award of Excellence: Omar Valdemar, CPP**
  Recognizes an ASIS member who has exhibited selfless devotion as a volunteer, emphasizing significant contributions at the community steering committee level over an extended period.
- **PCB Regional Certification Award: Abdullah Alshehri, CPP, PCI, PSP; Thamer Hussain Al-sufiani, CPP, PCI, PSP; Melvin Tze-Hui Cheng, CPP, PSP; Macky Diop, CPP; Daniel Jimenez; Tom Kipyegon, CPP, PCI, PSP; Jose Wilson Massa, CPP; Elroy Shirvington, CPP; Jason Michael Struck, CPP, PSP; Larry Woods, CPP, PSPP**
  Recognizes certified security professionals who have made significant contributions to the enhancement and advancement of the CPP, PSP, PCI, or APP designation.
- **I.B. Hale Chapter of the Year Award: Jamaica Chapter; Lima, Peru Chapter; Phoenix Chapter; and United Kingdom Chapter**
  Recognizes outstanding chapters that provide security practitioners timely and relevant resources, thus helping promote excellence in the security management profession worldwide.
- **Chapter Communications Award: Ukraine Chapter, Jamaica Chapter, and Singapore Chapter**
  Encourages establishment and improvement of overall communications to chapter members via website, newsletter, social media, email, or other forms of communication.
- **Outstanding New/Revitalized Chapter Award: Philippines Chapter**
  Recognizes chapters that have exhibited outstanding motivation, excellence, and service in chapters that have been in existence for fewer than five years or have been recently revitalized.
- **Chapter Community Service Award: Middle Tennessee Chapter and New Delhi, India Chapter**
  Recognizes an outstanding community-based activity that complements and supports the goals and purposes of ASIS International while increasing chapter awareness within the local community.
- **PCB Organizational Award of Merit: KAUST Government Affairs & Security**
  Recognizes an organization displaying outstanding leadership and commitment to professional development of their own security professionals through certification.

For more information about ASIS awards and to view honorable mentions, visit *asisonline.org/awards*.

Young Professionals Corner

In this issue, ASIS checks in with Young Professionals Community Global Outreach Chair McLean Essiene, CPP, PCI, PSP, and Community Engagement Vice-Chair Mirza Sheraz Altaf, CPP.



McLean Essiene, CPP, PCI, PSP

The ASIS Young Professionals Community provides a strategic entry point into an exciting career in the security industry. It grooms young professionals to be competent business leaders via strategic networking with peers and industry leaders, valuable mentoring under the guidance of established senior security executive ASIS members, and structured education via customized educational channels. Active participation and ongoing industry education—including board certifications—are critical for gaining experience and building confidence.

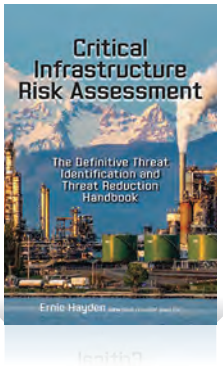
Mirza Sheraz Altaf, CPP

I initially thought that security is just a profession for those who retired from the military, police, and other armed forces. In reality, I've met people with backgrounds ranging from safety to information technology to engineering and more. I love this great mix of professionals in the security industry. Everybody has something different and unique to offer and share.

Security Industry Book of the Year

ASIS International's 2021 Security Industry Book of the Year is Critical Infrastructure Risk Assessment *by Ernie Hayden, PSP.*

"This book does a thorough job of explaining the various components of critical infrastructure and the definition of risk and risk management well enough to enlighten someone new to the subject or to reinforce the knowledge of a skilled security specialist with many years of experience in the field," said Joshua Fowler, CPP, in a book review in the July/August issue of *Security Management*. "It can easily be used as an instruction manual for conducting infrastructure vulnerability assessment training and a ready reference for ensuring thorough and complete assessments by experienced practitioners. A copy of this book should be on the shelf of any security professional performing these duties."



Now in its eighth year, the Security Industry Book of the Year is selected by a panel of ASIS members who review member-authored titles using criteria including relevancy to today's security threats, importance of the subject in the field, and the uniqueness of the coverage of a new security concept, idea, or technology.

Runners-up for the 2021 award include the seventh edition of *Effective Security Management* by Charles Sennewald and Curtis Baillie and the second edition of *Cybersecurity Law, Standards, and Regulations* by Tari Schreider.

"*Critical Infrastructure Risk Assessment* is the culmination of author Ernie Hayden's decades of experience assessing and protecting the can't-fail organizations responsible for national security and public safety," says Jennifer Hesterman, chair of the ASIS Book of the Year committee. "As threats to critical infrastructure abound and evolve, risks must be continuously evaluated and security planning and activities tailored accordingly. This extremely well-written and easy to digest book is mandatory reading for everyone working in a critical infrastructure sector, from seasoned managers to new employees on the front lines." ■

Judicial Decisions

Sabotage. A pharmacist who admitted to tampering with COVID-19 vaccine vials at his work received a three-year prison sentence.

Steven Brandenburg pled guilty to two counts of attempting to tamper with consumer products with reckless disregard for intentionally removing a box of Moderna vaccine doses from an Aurora Medical Center refrigeration unit for hours during two of his overnight shifts in December 2020. To remain viable, the vaccine needs to be stored at specific cold temperatures, and this information—along with other specifications on proper storage and use—was available to Brandenburg and other employees.

"Brandenburg is skeptical of vaccines in general and the Moderna COVID-19 vaccine specifically," according to court documents. Despite his education, the additional information provided by the U.S. Food and Drug Administration, and professional familiarity with the potential health consequences of improperly storing any vaccine, Brandenburg removed the doses and returned them to refrigeration. They were later distributed and administered to individuals at a clinic.

Besides admitting to coworkers that he was skeptical about vaccines, Brandenburg's actions were at least partly detected by a pharmacy technician who discovered the vials outside of a refrigeration unit.

After the hospital invited the FBI and other federal and local authorities to investigate the issue, Brandenburg admitted to his actions.

Brandenburg's sentence includes three years of supervised release and restitution of $83,829.05 to be paid to the hospital. (*United States v. Steven Brandenburg*, U.S. District Court of Eastern District of Wisconsin, No. 21-cr-0025-bhl, 2021)

Identity theft. To settle allegations of credit fraud and identity theft, smart home security and monitoring company Vivint Smart Home, Inc., agreed to pay $20 million to the U.S. Federal Trade Commission (FTC).

Vivint allegedly improperly used credit reports to qualify potential clients for financing and failed to set up and adhere to an identity theft program, according to an FTC press release. Sales representatives used various processes to approve others for loans for their services, including asking customers to give the name of someone known to them with a better credit rating and adding that person as a co-signer without his or her consent and "white paging"—where another customer with the same or similar name is found and used to qualify the hopeful customer. The customers whose identities were stolen were contacted by debt collectors about payments for additional products or services they never requested.

This settlement marks the largest financial settlement under the Fair Credit Reporting Act. Of the total fine, the civil fine amounted to $15 million, and the remainder was compensation to impacted customers. Beyond the financial penalties, Vivint must enact an identity theft prevention program, an employee monitoring and training initiative, and a customer service task force responsible for verifying that an account corresponds to the correct client before sending an account to a debt collector. (*United States v. Vivint Smart Home, Inc.*, U.S. District Court of Utah, No. 2:21-cv-00267-TS, 2021)

Legislation

U.S. States

Doxxing. Colorado Governor Jared Polis signed legislation into law that bans the sharing of personal information of public health workers or their families if the motivation is to harass or threaten them.

The Protections For Public Health Department Workers (formerly CO HB1107) expands protections for public health employees and contractors, allowing them to request their personal information—including addresses, photographs, and telephone numbers—be removed from on-

LEGAL HIGHLIGHTS

COURT CASES

Issue: Money laundering
Case: *United States v. Bank Julius Baer*
Venue: U.S. Dist. Ct., E.D. New York
Status: Settled
Significance: Bank will pay more than $79 million for conspiring to launder bribes with FIFA.

Issue: Carbon emissions
Case: *Milieudefensie et al. v. Royal Dutch Shell*
Venue: District Court of The Hague
Status: Ruled in favor of Milieudefensie
Significance: Shell must reduce greenhouse gas emissions 45 percent by 2030.

Photo by iStock; Photo illustration by *Security Management*

line public records. Individuals who publish this information with malicious intent could face up to 18 months in jail and a $5,000 fine.

The new law was enacted after an increasing number of threats were made against public health employees and contractors in 2020 while the COVID-19 pandemic spread. The protections mirror those already in place for law enforcement officials, human services workers, and their families in Colorado.

Doxxing, the online search for or publishing of personal information, can lead to online and in-person harassment and attacks. Doxxing can have various motives and consequences, including celebrity doxxing, which focuses on a celebrity's personal life; revenge or vigilantism; and erroneous doxxing, where the wrong person is linked to a group or situation.

China

Data security. The Data Security Law (DSL) of the People's Republic of China went into effect on 1 September 2021.

The DSL regulates all activities in China that involve data processing, including collection, storage, use, transmission, disclosure, refining, and provision. It also regulates data activities of people and organizations outside of China considered a national security threat or public interest.

The law requires national security agencies to create a National Data Security Coordination Mechanism, which will promote data security risk information sharing between agencies. It also creates a new category of data—national core data—which includes information related to the country's national security, economy, citizens' livelihoods, and essential public interests.

Regulations

United States

Discrimination. The U.S. Equal Employment Opportunity Commission (EEOC) clarified that companies may require employees to receive COVID-19 vaccines. The only stipulation is that the employer should not offer potentially coercive rewards for vaccination if it is administering the doses itself.

If an employee has a disability or sincerely held religious beliefs, practices, or observances that conflict with getting vaccinated, the employer must "provide reasonable accommodations," according to the EEOC guidance.

The guidance was issued in response to questions about whether such a requirement was a form of discrimination.

Hazardous conditions. The U.S. Occupational Safety and Health Administration (OSHA) fined six construction contractors in New Jersey and Pennsylvania for four willful and 35 serious violations.

OSHA said the contractors exposed employees to falls more than 6 feet and failed to provide personal protective equipment to workers at a luxury single-family home construction site. The incidents, which were observed during three separate inspections of the site, were violations of federal requirements to prevent falls in the workplace.

The penalties amounted to more than $244,000, and the contractors were also ordered to correct or contest each violation within 15 working days of the citation.

Disclosure. First American Financial Corporation agreed to pay the U.S. Securities and Exchange Commission (SEC) a $487,616 to settle charges linked to a 2019 data breach.

The real estate title insurance company allegedly failed to disclose a weak point in its cybersecurity, which resulted in the compromise of more than 800 million images of documents. The data included Social Security numbers and bank account statements.

Although the firm's information security staff detected the leak in January 2019, the SEC said the company waited roughly four months before disclosing it. Meanwhile, the problem remained, and company leaders were not informed. (*In the Matter of First American Financial Corporation, U.S. Securities and Exchange Commission*, No. 3-20367, 2021) ■

International Legislation

United Kingdom

Domestic abuse. Queen Elizabeth II gave Royal Assent to allow the Domestic Abuse Act 2021 to become law. It widens the definition of domestic abuse to include coercive or controlling conduct, emotional abuse, and financial abuse, as well as physical violence.

The law also offers additional protections to domestic abuse victims in civil and family courts, including giving them protective screens, the option to testify through a video link, and prohibiting accused abusers from directly cross-examining their victims. Children who witness any abuse are now explicitly recognized as victims.

The act gives law enforcement additional powers, including being able to provide victims with immediate protection from abusers with Domestic Abuse Protection Notices and Orders. The latter requires offenders to seek either mental health support or rehabilitation for substance abuse.

Other changes created by the act include the banning of the "rough sex" defense, which allowed accused abusers to claim that violent acts were consensual; criminalizing threats of sharing private sexual photographs and films with the intent to cause distress, sometimes known as revenge porn; and making non-fatal strangulation a specific offense with attackers facing a maximum sentence of five years in prison.

Previously, incidents of non-fatal strangulation could result in attackers being charged with common assault, which carried a maximum jail sentence of six months.

Issue: Espionage
Case: *United States v. Peter Debbins*
Venue: U.S. Dist. Ct., E.D. Virginia
Status: Sentenced
Significance: Debbins sentenced to 188 months in federal prison for sharing military secrets with Russia, violating the Espionage Act.

Issue: Fraud
Case: *VZBV v. Daimler AG*
Venue: Stuttgart Higher Regional Court, Germany
Status: Filed
Significance: Daimler accused of manipulating diesel vehicle emissions data.

Issue: Cybersecurity
Case: *Van Buren v. United States*
Venue: U.S. Supreme Court
Status: Ruled in favor of Van Buren
Significance: Narrowed the scope of the Computer Fraud and Abuse Act.

MARKETPLACE

Included in this month's solutions are PoE testers, video management software, dust covers, and more.

#901

Video Management

VIVOTEK announced an update to its VAST 2 IP video management software solution. The update includes easy operation on single or multiple monitors, a custom layout for accommodating corridor and panorama orientations, fast export of multichannel video, and incorporation of VCA analytics and cybersecurity attack events from VIVOTEK cameras and substations. Other new features include an access control solution and evidence image of LPR cameras.

www.vivotek.com

#902

Crime Prevention

Interface Security Systems announced its artificial intelligence-based Anti-Loitering System. The solution uses AI in its object detection system, deterring people and vehicles from loitering with pre-recorded, scenario-specific voice messages. Intended for after-hours perimeter control challenges—including vagrancy, intrusions, and vandalism—a client's loss prevention team can customize this solution to play up to four individual warnings and notification messages depending on the location and time. Although it can operate as a standalone system, it can also integrate with an intrusion alarm system with remote monitoring or with Interface's virtual guard service for real-time remote operator intervention.

www.interfacesystems.com

#903

PoE Tester

Platinum Tools announced the launch of its new pocket-sized PoE++ tester, the TPS200C. The tester was designed for all types of Power over Ethernet (PoE), including up to 56 volts and 280 watts of power. It requires no batteries and is instead powered by the PoE circuit, so it can be used inline with a PoE device to measure current flow or by itself in Powered Device Simulation mode, allowing users to determine the maximum power available from the PoE power source. The tester can also test up to 4-pair PoE, offers an easy-to-read OLED display, and can test PoE on active data cables without interrupting a data flow.

www.platinumtools.com

#904

Dust Covers

A new product from ABLOY USA Critical Infrastructure provides a solution to additional safeguarding efforts against environmental conditions. The IP54-rated Integrated Dust Cover offers an internal shield specifically designed for the ABLOY mechanical and PROTEC2 CLIQ cylinders. The cover protects locks' internal components with a built-in spring-loaded shutter that blocks the key opening when not in use, reducing exposure to the elements. The dust cover also improves resistance to environmental wear and corrosion from dirt, moisture, and freezing conditions.

www.abloyusa.com

#905

Operating Platform

Senstar introduced its Symphony Common Operating Platform as a scalable modular solution for video management, security management, data intelligence, access control, and perimeter intrusion detection. The platform, which offers a sensor fusion engine and built-in video analytics, also includes full-featured access control and perimeter intrusion detection modules. The modular format allows for each function to be used individually, as well as coexist with third-party systems. The platform offers per device licensing with the option to add licenses at any time, plus it includes a built-in server and database redundancy.

www.senstar.com

REQUEST DETAILED PRODUCT INFORMATION THROUGH OUR MONTHLY E-RESPONSE, VISIT HTTP://SECURITYMGMT.HOTIMS.COM, OR USE YOUR SMARTPHONE TO ACCESS THE QR CODE ON THIS PAGE.

1. Download a free QR code reader from the Android, Blackberry, or iPhone apps store.
2. Open the app, hold your phone camera steadily above the QR code on this page, and your device will connect to our custom site where you can request product information from any of our advertisers.

CIRCLE #		PAGE #
-	AirAccess/Napco	Corner Peel
08	Ameristar	19
04	AXIS Communications	08
14	Brownyard Group	31
18	CEIA Ferromagnetic	51
07	CEIA	15
131	Continental Access/Napco	S16
10	Comnet	23
03	Detex	06
11	Garret Metal Detectors	25
13	Genetec	27
01	Hanwha Techwin	SPLIT COVER
102	Marks USA/Napco	S02
19	Mission 500	69
17	Morse Watchmans	45
12	Par-Kut International	26
02	Prosegur	04
06	Special Response Corporation	13
05	Speco Technologies	11
20	StarLink Fire LTE/Napco	70
130	TEAM Software	S15
15	Zbeta Consulting	33

*** Supplement denoted in orange.**

advertisers online

AirAccess/Napco
www.airaccesscontrol.com

Ameristar
www.ameristarsecurity.com

AXIS Communications
www.axis-communications.com

Brownyard Group
www.brownyguard.com

CEIA
www.ceia.com

CEIA Ferromagnetic
www.ceia-fmd.com

Continental Access/Napco
www.cicaccess.com

Comnet
www.comnet.net

Detex
www.detex.com

Garrett Metal Detectors
www.garrett.com

Genetec
www.genetec.com

Hanwha Techwin
www.hanwhasecurity.com

Marks USA/Napco
www.marksusa.com

Mission 500
www.mission500.org

Morsewatchmans
www.morsewatchmans.com

Par-Kut International
www.parkut.com

Prosegur
www.prosegur.us

Special Response Corporation
www.specialresponse.com

Speco Technologies
www.specotech.com

StarLink Fire LTE/Napco
www.starlinklte.com

Team Software
www.teamsoftware.com

Zbeta Consulting
www.zbeta.com

The Domino Effect

The COVID-19 pandemic created critical shortages of basic food necessities worldwide. Workers were unavailable to harvest produce, and supply chains stalled. When facing a lack of genuine or affordable raw material, INTERPOL and Europol's *Operation OPSON IX Analysis Report* found that dishonest producers used low quality or unsuitable ingredients, resulting in "an increase of illegal, counterfeit, and potentially unsafe food on the market."

Results

The number of checks is only 39 percent of the amount reported in the previous year's OPSON results, while criminal cases are a mere 13 percent of the OPSON VIII rate. COVID-19 and lockdown measures—as well as supply chain transportation difficulties—most likely affected criminals, and countries.

27,579
Checks

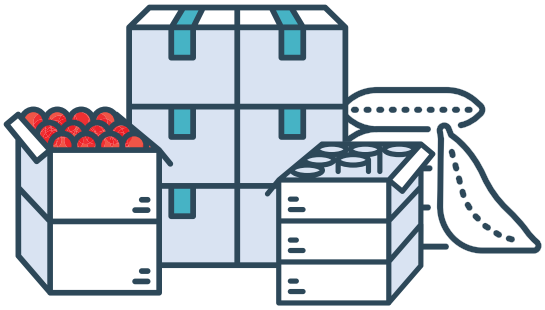
407
Arrests

19
Organized Crime Groups Disrupted

Illegal and Potentially Harmful Products Seized

12,000 Tons
of product seized, including

2 Million
liters of fake and substandard drinks



Most Seized Items

Raw Animal Feed

Unregulated raw animal feed could affect the entire food supply chain, the report found.

Alcoholic Beverages

Most of the alcohol seized was wine, followed by vodka and whiskey.

Intellectual Property Infringements

Whether related to trademark, copyright, or geographic indications of origin, intellectual property rights were violated in 132 reports during Operation OPSON, mostly in connection with alcoholic beverages, condiments, and meat products.

8%
of total seizures were related to counterfeiting.

Infographic design by Mariah Bartz; Illustrations by iStock

Support a School in Your Community
Host a Care Pack Build with Mission 500

The cost of school supplies has risen dramatically this year, making an already difficult situation for children in need returning to classrooms even more challenging. Help support children in your immediate community by sponsoring a Care Pack Building Event with Mission 500. Companies of all sizes – even individuals – can sponsor an event with help from friends, family and the community with support from Mission 500's experienced team of fund raising specialists.

Find out how you can make a difference in the lives of children where you live.

Learn more by visiting mission500.org/care-pack, emailing kat@mission500.org or calling 207-500-7103.

Supporting Families Across America

MISSION500

Don't Wait Until It's Too Late

Save Lives & Money. Replace POTs lines on Fire Alarms Today with Leading Fire Cellular for All FACPs

AT&T® or verizon✓®

- **Safeguard All Fire Alarms Now In Jeopardy Of Failing To Communicate as weather, events or Telephone Companies continue to cut off leased landlines – *Tradeup to StarLink Cell Communicators for less***
- **Improve Alarm Response Times When Seconds Matter Most, Save Life And Property with StarLink Fire® fast cellular reporting to any Monitoring Station**
- **Proven to Save $1000'S Of Annual Budget Dollars vs. POTs lines –** Each Starlink Fire Cell Communicator replaces 2 leased landlines per FACP
- **AHJ-Friendly & Code Compliant: NFPA 72 2019, UL 864 10th Ed, CSFM, LAFD, NYC FD**
- **Supports All FACP brands, 12V or 24V, new or old –** StarLink Panel-Powered Technology installs in minutes; Low current draw, NO additional power supply & NO extra conduit. Dual Path Cell/IP now with EZ-Connect Telco jacks & self-supervised w/o modules.
- **AT&T or Verizon StarLink models to choose from, proven to work, even where others won't,** using Signal Boost™ & twin dual diversity antennae for max. signal acquisition & null avoidance, *not possible with single stick antenna radios*

See us at GSX, NAPCO Booth 1218

NAPCO StarLink Fire

1.800.645.9445 • www.StarLinkLTE.com

StarLink, StarLink Fire™, Signal Boost™ are trademarks of Napco. Other marks trademarks of their respective cos. †For model compliance listings always consult tech docs & AHJ.