SECURITY MANAGEMENT

AUGUST 2020

A PUBLICATION OF ASIS INTERNATIONAL

Issue & Beyond

× ***Corruption***
Emergency pandemic funding efforts endanger transparency.

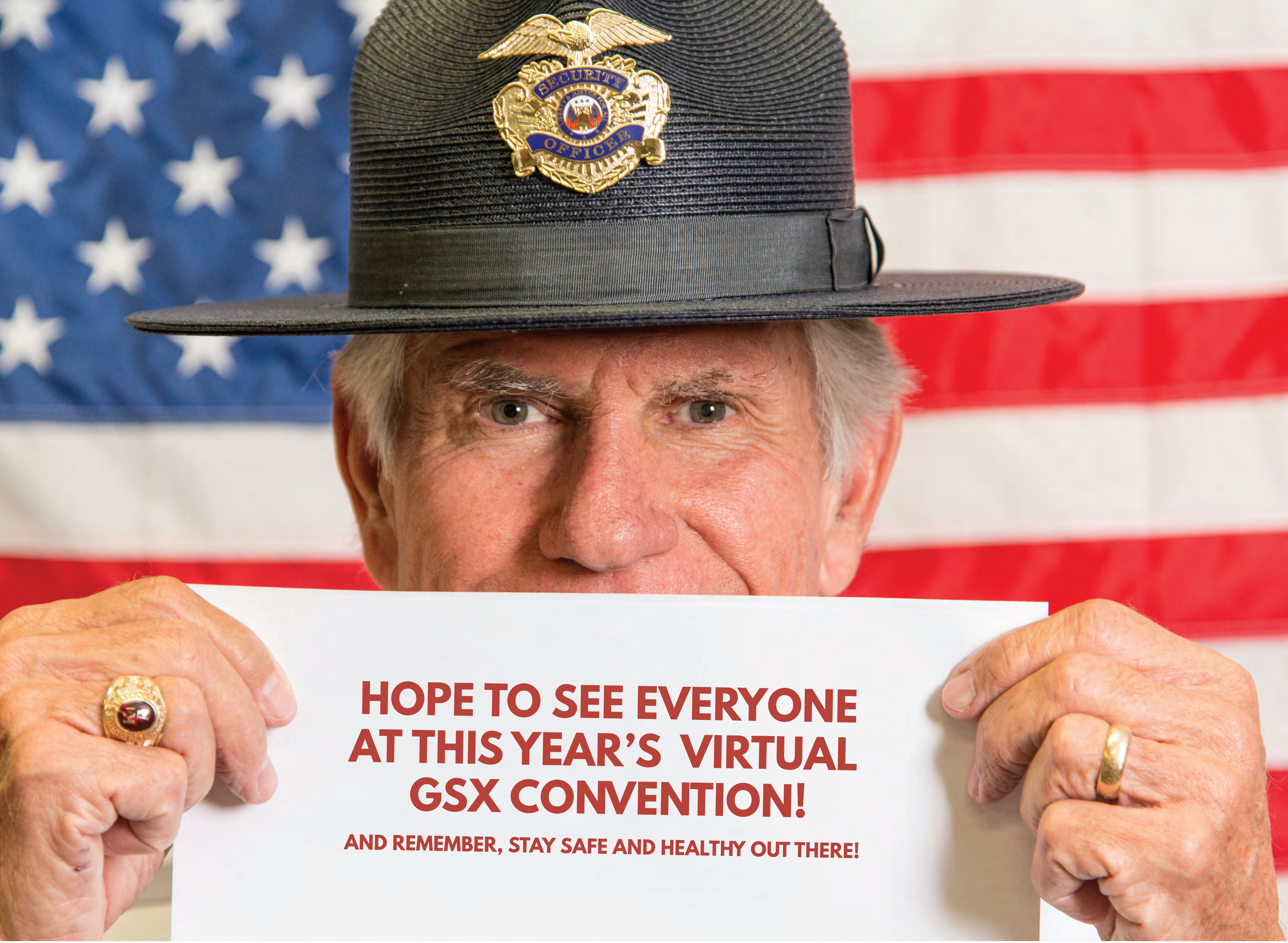
× ***Terrorism***
Despite recent losses, Islamic State threats persist.

×38
CRITICAL INFRASTRUCTURE

×44
SUSTAINABLE SECURITY

×48
CONTEXTUAL INTELLIGENCE

×30
STUDENTS IN
DISTRESS


SECURITY
OFFICER
HOPE TO SEE EVERYONE
AT THIS YEAR'S VIRTUAL
GSX CONVENTION!
AND REMEMBER, STAY SAFE AND HEALTHY OUT THERE!

For over 25 years, the GSX convention has been one of my favorite events. Although I will miss seeing the ASIS members again this September, I understand that pivoting to a virtual conference this year is the right call. As security management professionals, I challenge you all to remain steadfast in supporting each other and sharing industry knowledge during these complex times when our services are more critical than ever.

As the future effects of COVID-19 remain unclear, our primary focus at SecurAmerica is to ensure our employees remain safe at our 320 offices across the US. We are also committed to partnering with our customers as they are facing their own increasing obstacles. Our heritage is Legendary Service, and we are honored to continue serving our local communities as we emerge from this crisis together.

My thoughts are with you all, and if you have any questions you can reach me directly at 404-926-4202.

SECURAMERICA
WWW.SECURAMERICALLC.COM

100R-6522901/A120

AUG 2020

CONTENTS

NOTABLE

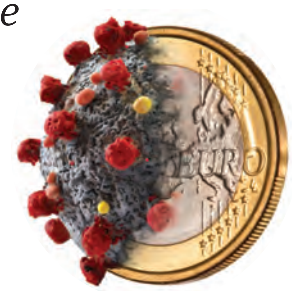
2/3

of the 40,000 aspirant foreign fighters who joined the ISIS caliphate may still be alive, posing a long-term, international threat, according to a United Nations report. **PAGE 21**

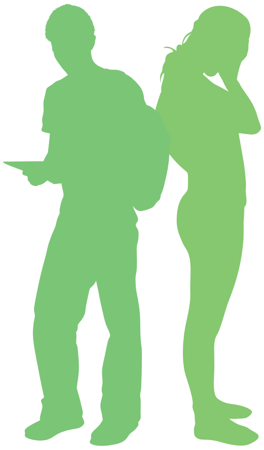
86

The percentage of reported data breaches in 2019 that were carried out for financial gain. **PAGE 27**

"In a time of crisis, when resources are scarce and the stakes are high, eliminating corruption in the response to an emergency is literally a matter of life and death."



Irem Röntgen discusses fraud subverting COVID-19 pandemic relief efforts. **PAGE 16**



"The situation's already tense enough without us raising the anxiety level."

Rick Gilbert explains how empathy and de-escalation can address students' pandemic-triggered stress. **PAGE 36**

19,000

The number of artifacts recovered in a 103-country art trafficking crackdown. **PAGE 18**

IMAGES BY iSTOCK

Security Management (ISSN 0145-9406) Volume 64, Number 8, is published monthly 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. Statements of fact and opinion are made on the responsibility of the authors and do not imply an opinion on the part of the editors, officers, or members of ASIS. Advertising in this publication does not imply endorsement or approval by *Security Management* or ASIS. The editors reserve the right to accept or reject any article or advertisement. Quantity reprints of 100 or more copies of each article may be requested from *Security Management* Reprints Dept. at 703.518.1451.

HID

AUGUST 2020

ASIS INTERNATIONAL
Advancing Security Worldwide®

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

Nello Caramat
publisher
Nello.Caramat@asisonline.org

BUSINESS OFFICES
1625 Prince Street
Alexandria, VA 22314
703.519.6200
fax 703.519.6299

SALES REPRESENTATIVES

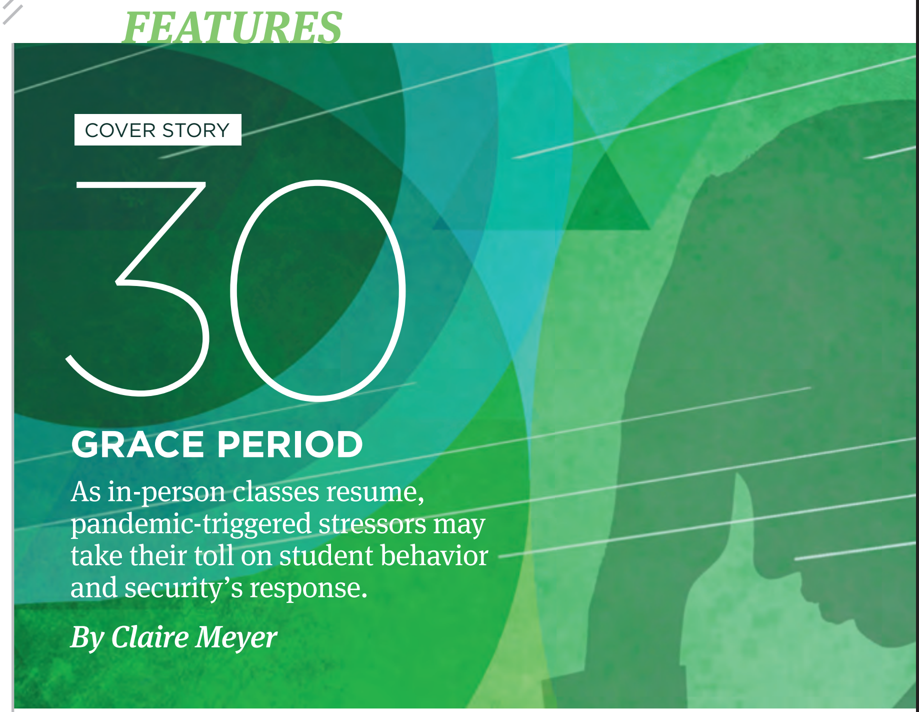
Southern/Mid-Atlantic & Europe media sales manager
Shawn Register
703.518.1492
Shawn.Register@asisonline.org

Northeast/Midwest/West Coast media sales manager
Charlotte Lane
703.518.1510
Charlotte.Lane@asisonline.org

On the Cover:
Illustration
by Stephanie Dalton Cowen

CONTENTS

FEATURES



ASIS FOUNDATION DIGITAL TRANSFORMATION SERIES

ASIS FOUNDATION

BLOCKCHAIN:
A GUIDE FOR SECURITY PROFESSIONALS

AUGUST 2020

SECURITY MANAGEMENT

EDITORIAL STAFF

Teresa Anderson
editor-in-chief
Teresa.Anderson@asisonline.org

Claire Meyer
managing editor
Claire.Meyer@asisonline.org

Megan Gates
senior editor
Megan.Gates@asisonline.org

Sara Mosqueda
assistant editor
Sara.Mosqueda@asisonline.org

Flora Szatkowski
editorial assistant/staff writer
Flora.Szatkowski@asisonline.org

PRODUCTION & CREATIVE SERVICES STAFF

Tyler Stone
art director
Tyler.Stone@asisonline.org

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

Caitlin Donohue
graphic designer
Caitlin.Donohue@asisonline.org

Mariah Bartz
graphic designer
Mariah.Bartz@asisonline.org

Matthew Kreider
publishing specialist
Matthew.Kreider@asisonline.org

EDITORIAL OFFICES

1625 Prince Street
Alexandria, VA 22314
703.519.6200
fax 703.519.6299

EDITORIAL

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.

CONTENTS

DEPARTMENTS

ILLUSTRATION BY *SECURITY MANAGMENT*; iSTOCK

CHECK OUT MORE ONLINE
at *securitymanagement.com*

CONTRIBUTING *AUTHORS*

DIANA M. CONCANNON

ASSOCIATE PROVOST
ALLIANT INTERNATIONAL UNIVERSITY

Diana M. Concannon is associate provost for strategic initiatives and partnerships at Alliant International University, where she also serves as dean of the California School of Forensic Studies. She has more than 25 years of executive leadership experience to support the development and delivery of practical, accessible education for practitioners in the public safety, security, and mental health sectors.

Concannon maintains a threat assessment and management consultancy. She is the author of *Kidnapping: An Investigator's Guide to Profiling* and *Neurocriminology: Forensic and Legal Applications, Public Policy Implications*. For ASIS International, she is special advisor to the Professional Development Council and a member of the School Safety and Security Council.

"Security in Context" **PAGE 48**

MICHAEL CENTER

REGIONAL SECURITY ADVISOR
UNITED NATIONS

Working for the United Nations Department of Safety and Security, Michael Center is security advisor to Belgium, Finland, Germany, Ireland, Malta, Monaco, Norway, Portugal, Spain, Sweden, and the United Kingdom. His experience is focused on security risk management in high-risk, complex environments. He serves as liaison from the United Nations to the ministries of interior and defense of host governments to share information to strengthen analysis and crisis management.

Center is the chair of the ASIS International Professional Development Council and co-vice chair for subject matter expertise on the ASIS Council on Global Terrorism, Political Instability, and International Crime.

"Security in Context" **PAGE 48**

MARK H. BEAUDRY, CPP | RESEARCHER AND WRITER | SECURITY STUDIES

Mark Beaudry has been a member of ASIS International since 1982 and a Certified Protection Professional (CPP®) since 1996. He is a frequent researcher and author in security studies, police education and performance, criminology, and the history of the Middle East.

A retired intelligence chief, area studies analyst, Marine security guard, and certified anti-terrorism instructor for the U.S. Marine Corps Reserve, Beaudry holds a PhD in Human Services/Criminal Justice.

Book Review **PAGE 17**

DANTÉ MORICONI, CPP, PCI, PSP | PHYSICAL SECURITY MANAGER | L3 HARRIS TECHNOLOGIES, INC.

Danté Moriconi, CPP, PCI, PSP, CFE (Certified Fraud Examiner), is physical security manager for the Broadband Systems Sector of L3 Harris Technologies in Salt Lake City, Utah.

Moriconi has been an active ASIS International member, serving in multiple roles on the Physical Security Council, as well as in local chapter leadership.

Book Review **PAGE 21**

DANIEL BENNY, CPP, PCI | ASSOCIATE PROFESSOR | EMBRY-RIDDLE AERONAUTICAL UNIVERSITY

Daniel Benny holds a PhD in Criminal Justice and is a tenured full-time associate professor in Intelligence and Security Studies at Embry-Riddle Aeronautical University Worldwide Campus. He is the author of seven textbooks on security matters and has been a member of ASIS International since 1976.

Benny is a graduate of the Naval War College and the U.S. Air Force Air University Air War College.

Book Review **PAGE 27**

ERNIE VAN DER LEEST | CORPORATE SECURITY MANAGER | MUSE ENTERPRISES

Ernie Van der Leest is a retired 28-year law enforcement officer with experience in patrols, training, K9, digital forensics, and criminal investigations.

Van der Leest is a member of the ASIS Investigations Council and the Law Enforcement Liaison Council. He co-authored a publication related to interview room design and has conducted thousands of information and in-custody interviews involving cases ranging from theft to capital murder.

Book Review **PAGE 58**

As you strive to keep employees and visitors safe in this new normal, we are bringing together the latest technology to help you reopen your workplace with confidence.

Explore solutions for your organization at **adtcommercial.com** or call **855-ADT-COMM**

ADT® Commercial

For product info #5 securitymgmt.hotims.com

SM DIGITAL

TOP TWEET

Privacy and human rights should always take center stage when considering how technology should be employed, one facial recognition technology developer writes in the June issue of *Security Technology.*

Security Management @SecMgmtMag · Jun 9

Privacy and human rights should always take center stage when considering how technology should be employed, one facial recognition technology developer writes in the June issue of Security Technology.

Should Facial Recognition Be Banned?

In a time of crisis, it's tempting to let down our guard about surveillance. But privacy and human rights should always take center stage when ...

asisonline.org

TOP POST

In a crisis, safe shelter is critical. Here's how security managers at hotels are adapting to threats to keep guests safe during their stay.

Security Management Magazine

Published by Megan Gates [?] · June 8 at 10:50 AM ·

In a crisis, safe shelter is critical. Here's how security managers at hotels are adapting to threats to help keep guests safe during their stay.

ASISONLINE.ORG

Safeguarding Your Stay: Hospitality Security Risk Management in Unique Situations

COMMENTS

"This is very serious, especially in our profession where we and our teams have been exposed to stressful situations." —Leopoldo Morales, security and safety head, Argentina, DHL Express, on the June *SM* article "Battling Burnout."

SM ONLINE

FRAUD

Corruption in the health sector causes losses of more than $500 billion every year, according to Transparency International.

COVID-19 SCAMS

In late May, the U.S. Federal Trade Commission announced it had received more than 52,000 reports of COVID-19 related scams since the beginning of 2020.

STUDENT SAFETY

By the end of April, fewer than 40 percent of students surveyed by the American Civil Liberties Union of Southern California rated their mental wellness at pre-pandemic levels.

CYBERATTACKS

In an audit, the U.S. Government Accountability Office found that the electric grid is increasingly vulnerable to cyberattacks—especially those involving any industrial control system that supports grid operations.

INDUSTRIAL CONTROL

Dragos—a security firm specializing in industrial control system (ICS) protection—reported that the amount of activity targeting ICS increased significantly in 2019.

@ Go to SM Online for these and other links mentioned throughout this issue.

CURRENT PODCASTS

In July's episode, Sandra Stibbards explains security hygiene basics to avoid intellectual property theft attempts, and Glenn Kitteringham, CPP, breaks down active versus passive learning within security guard training programs.

TRENDING ARTICLES

1 **DIGITAL TRANSFORMATION**
Microsoft's VSOC Revs Up During COVID-19
By Claire Meyer

2 **PROFESSIONAL DEVELOPMENT**
Security Career Paths: Preparing for Personality Assessments
By Thomas R. Stutler, CPP

3 **HOSPITALITY**
Safeguarding Your Stay: Hospitality Security Risk Management in Unique Situations
By Erik Antons, CPP, PSP

We're proud to welcome Christina Duffey to our team.

But we're even more proud to tell you why she chose us.

At PalAmerican Security, we put an emphasis on people, culture, and values. Whether it is developing our employees through industry leading training programs and promoting from within, or listening to our clients' needs and creating a program to exceed them, we put people first. And it's because of these strong values that Christina Duffey decided to join PalAmerican Security. With Christina, we've gained someone with 30 years of industry experience who will help drive our business forward and assure your safety and peace of mind.

We're here to help.
Contact us today for a free consultation:
PALAMERICAN.COM

PalAmerican
★★★★★★★★★★★★★★★★
SECURITY

Paladin Security

Paladin Risk Solutions

Paladin Technologies

For product info #6 securitymgmt.hotims.com

Editor-in-Chief
TERESA ANDERSON

APPEARANCES

"There may be times and places where it is a good idea to talk back to a military officer, but Germany in 1906 isn't one of them." So begins Tim Harford's recounting of "The Captain of Kopenick," a well-known tale about fraudster Wilhelm Voigt. In the episode "The Rogue Dressed as a Captain" from his podcast *Cautionary Tales,* the author and columnist for the *Financial Times* discusses how the human brain tends to trust the appearance of authority, and that once a person embarks on a path, it is difficult to change course.

Voigt impersonated a captain and convinced two squads of German soldiers to board a train, ride from Berlin to the town of Kopenick, and arrest the town's mayor. During the arrest, Voigt seized the town's funds—the equivalent of $250,000—on suspicion of fraud. The soldiers took the mayor to jail while Voigt changed into civilian clothes and escaped with the money.

The details of this story are revealing, says Harford. Voight approached the squad leader dressed in an officer's uniform and asked where he was going. The leader naturally answered this innocent question. Voigt then asked the squad to follow him, on orders from "the highest level." What was the harm in marching down the street, especially if ordered to by senior officials? By the time Voigt encountered the second squad of soldiers, he had a squad following him already, so the second squad naturally fell in line.

When the soldiers forced their way into the town hall, they might have had second thoughts, notes Harford, but by then it would have been difficult to challenge the situation. It had gone too far.

Diana Concannon and Michael Center recount a similar anecdote in their article, "Security in Context," in this month's issue. An expensive, well-planned security program at a Tokyo facility was thwarted by a color printer, a fake badge, and a very convincing red team member. The penetration tester told building staff that he had flown in from the United States for an emergency audit at the insistence of the CEO.

Similar to the squads' response to Voigt's tactics, the staff on duty defaulted to an appearance of authority, and let the tester into the building.

Concannon and Center contend that understanding this tendency—along with culture, organizational values, and politics—can help improve a company's security posture. They call this contextual intelligence and assert that it can be taught at all levels of the organization.

At the time of Voigt's exploits, Harford notes, the story was used to poke fun at the German people—they "were suckers for a shouty man in a uniform." Harford says this is unfair. We all fall for superficial things. We trust tall people more than short people. We trust people in lab coats, even if they tell us they aren't doctors.

Appearances matter. But so does context. If security professionals can train employees to overcome their biases, they can shift the thinking of the entire organization.

COVID-19: SECURITY RESOURCES

FEATURED RESOURCE

Key Risks to Split Operations Models

Separating key business groups by time, distance, or both can mitigate infection risks as organizations reopen. While this split operations strategy has many benefits, it also has a few key risks, as outlined by Prometheus Yang and Leslie Holland in their *Security Management* article "Implementing Split Operations to Improve Resilience During a Disease Outbreak."

Key person risk. If a business unit is too heavily reliant on one key individual and that employee becomes ill, it can have devastating consequences. Cross-training within business units—especially if units have divided into smaller working groups or staggered shifts during a split operation—can mitigate this risk.

Movement control. When using physical distancing measures, like splitting a business unit across two floors, employees may try to return to their original workspace, potentially cross-contaminating other groups.

In-person meetings. Eliminate face-to-face meetings whenever feasible to effectively sustain split operations. Organizations should encourage the use of virtual communication tools like messaging or video conferencing platforms to improve productivity and socialization.

Complacency. With practice, Yang and Holland write, what was once new can become routine. To reduce complacency risks, executives must lead by example or risk eroding employee trust.

SECURITY SNAPSHOT

"There's nothing quite like a good emergency or a good crisis to bring the best out of a security team and to test your processes. So of course, it's like trial by fire—the teams that are able to be agile, that are able to be responsive, that are immediately able to demonstrate cross-functional leadership…it is the molding of the appropriate security manager."—Nicole McDargh, CPP, regional director of physical security, health, safety, and building and offices services, for Richemont Europe, discusses emergency planning and leadership in a June ASIS Security Snapshot video.

IMAGES BY iSTOCK

WEBINAR

Crisis and Threat Management Considerations for Business Resumption Against the Backdrop of COVID-19 and Social Unrest

Although the COVID-19 pandemic forced many organizations to rapidly shift to remote work, returning to the workplace will require a more gradual approach.

Learn how to optimize business resumption planning in this on-demand webinar at *asisonline.org.*

LEARN MORE

Up-to-date statistics, news, and resources are available online at *asisonline.org/covid-19.*

ILLUSTRATION BY *SECURITY MANAGEMENT*; ISTOCK

PANDEMIC PROFITEERS

AS GOVERNMENTS RUSH TO ADDRESS THE CORONAVIRUS PANDEMIC, CHECKS AND BALANCES CAN BE LEFT BY THE WAYSIDE, PRESENTING TEMPTING OPPORTUNITIES FOR FRAUD AND CORRUPTION.

BY CLAIRE MEYER

IN THE WEST AFRICA Ebola outbreak of 2014–2016, the International Federation of Red Cross and Red Crescent Societies (IFRC) played a pivotal role in disease prevention. Teams of volunteers provided treatment and care, as well as burying victims of the disease, preventing as many as 10,500 additional cases, IFRC estimates. However, where there is money being spent on crisis response, there is opportunity for fraudsters to take action.

Transparency International warned that the influx of funds and donations into the region would make response efforts vulnerable to fraud and corruption. In a subsequent investigation, IFRC uncovered millions of dollars' worth of fraud across the humanitarian organization's operations in West Africa. Of the more than $124 million handled by the organization during the Ebola epidemic, approximately $6 million was lost through collusion between former IFRC staff and bank employees in Sierra Leone, overbilling and fake billing by a customs clearance provider in Guinea, and inflated prices for goods and services in Liberia.

Today, the wider scale of the coronavirus pandemic, which has touched six continents, also presents a wider stage for corruption, backroom deals, and fraud.

According to Transparency International, corruption in the health sector causes losses of more than $500 billion every year, even without the extreme circumstances of a pandemic. Health sector corruption often involves solicited informal payments from patients in exchange for treatment; theft and embezzlement of money, medicine, or medical equipment and supplies; favoritism for certain patient groups over others; and data manipulation, such as fraudulent billing.

"In a time of crisis, when resources are scarce and the stakes are high, eliminating corruption in the response to an emergency is literally a matter of life and death," says Irem Röntgen, business integrity program coordinator for Transparency International. "Yet, with large amounts of resources suddenly available and a rush to get it to those most in need, there are sadly still those who will seek to take advantage for their own benefit."

In the coronavirus pandemic, this behavior was quickly apparent. In late May, the U.S. Federal Trade Commission (FTC) announced it had received more than 52,000 reports of COVID-19 related scams since the beginning of 2020, resulting in almost $39 million in losses. The average consumer lost $470.

"Sadly, corruption often flourishes in times of uncertainty and could undermine the response to the pandemic," wrote Lisa Ventura, practice lead of the Partnering Against Corruption Initiative at the World Economic Forum, in a recent article. While the response to COVID-19 should focus on saving lives and addressing health and socioeconomic consequences quickly and effectively, she added, "principles of transparency, justice, and good governance need to underpin all measures at all times."

"Transparency and accountability must not be lost in the haste to respond to COVID-19," she wrote.

As governments enacted emergency legislation to bypass typical checks and balances on public spending to expedite health crisis response measures, transparency may have already been left by the wayside. According to a report by the Lawyers Council for Civil and Economic Rights at the Cyrus R. Vance Center for International Justice, *Corruption in Times of COVID-19: A Regional Perspective on Public Procurement*, corruption related to public procurement for pandemic response has been alleged in at least 12 countries across North and South America as of April 2020.

"While corruption risks always exist, the costs of these risks are higher during the emergency as already limited public resources are syphoned off due to corruption," the report warned. The lawyers' report highlighted misappropriation of public goods and increases in direct purchases and contracts for health-related equipment and services, instead of acquiring goods through more transparent public bid processes. These shifts may produce short-term results but long-term risks of increasingly corrupt government systems and national processes, which threatens both citizens and private organizations.

"Essentially, corrupt political systems become less responsive to the needs and interests of ordinary citizens," Röntgen says. "We see that countries with more corrupt public sectors have fewer opportunities for diverse groups to engage in decision making, for example. For businesses, this can mean that only those companies with close links to those in power are able to win contracts or take advantage of government incentives for the private sector."

In addition, some key materials—such as personal protective equipment (PPE)—have been in short supply in different regions affected by the pandemic. In the environment of high demand and low supply, governments, private companies, and individuals are forced to compete to gather the necessary PPE, leading opportunists and bad actors to take advantage of the situation to sell counterfeit or shoddy goods, price gouge, or seek favors or bribes.

According to the UN Office on Drugs and Crime, between 10 and 25 percent of all money spent on procurement globally is lost to corruption. In the European Union, 28 percent of health corruption cases are specifically related to medical equipment procurement, Transparency International reported.

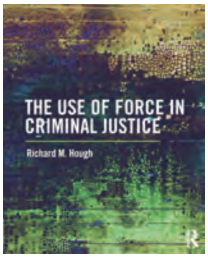
"Public procurement of emergency equipment has quickly emerged as an area to watch closely, as governments relax procurement regulations in order to quickly obtain essential goods," Röntgen says. "This opens the door for backhanders, price gouging, and conflicts of interest. It is essential that there is transparency about how governments are spending funds to fight the pandemic, so that any abuse can be identified and those responsible held accountable."

Writing for Pillsbury Law, Aaron Hutman, Jenny Sheng, and David Oliwenstein warn that the COVID-19 pandemic exposes a large number of organizations and individuals to legal risk, as well as the risks associated with falling prey to a scam or risking the purchase of ineffective PPE. "In the aftermath of the COVID-19 pandemic, we expect to see widespread enforcement actions by the U.S. government, other national governments, and multilateral development banks. Companies will face large penalties, and individuals who participated in unlawful activity or looked the other way may face criminal liability," they wrote.

USE OF FORCE

BY RICHARD M. HOUGH. Routledge; Routledge.com; 192 pages; $51.95

Current events underscore the importance of understanding "use of force." Dr. Richard Hough, who has a background in law enforcement, corrections, and education, employs useful examples to clearly illustrate and emphasize the concepts in *The Use of Force in Criminal Justice.* The book emphasizes the practical side of the issue and targets law enforcement managers.



Real-life examples are reviewed and analyzed so that readers cannot help but understand the lessons learned. Current best practices are explained for ensuring that incidents are thoroughly investigated at the time of occurrence. Because complaints and litigation can occur years after an incident, Hough illustrates his recommendations with actual litigation examples. Further, he addresses each point from a police officer's perspective, with advice on how to prevent, manage, and minimize use of force incidents.

The author emphasizes the importance of balancing policy and procedure, as well as how to properly investigate and discipline an officer who uses excessive force. He also provides ample material on how to support and defend officers when they act within the law and correctly follow procedures. There is also coverage of topics such as memory distortions and recall; chain of command responsibilities; and fair, detailed, and open investigations.

This book is a good reference for law enforcement and security management, police academies, and both proprietary and contract security organizations. It is also a good in-service training resource. Every public and private officer, supervisor, and executive will benefit from the concepts and recommendations in this book. The information provides insight for classes in any security studies or liberal arts criminal justice program. Anyone interested in a law enforcement or security profession as a career should read this book to better understand the decisions that have to be made on the job every day.

REVIEWER: *Mark H. Beaudry, CPP, is a frequent reviewer for* Security Management *and a longtime member of ASIS.*

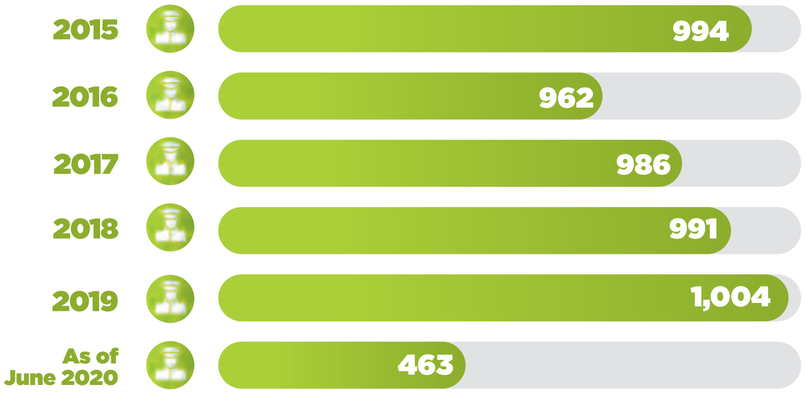
"At some point in the next 12 to 24 months, the world will return to some level of economic normalcy. Politicians, the media, watchdogs, and whistleblowers will begin to shine daylight on the activity that took place during the chaos of the pandemic. If past crises are any guide, public outcry for accountability will ensue," they added.

"In one sense," Röntgen notes, "COVID-19 will be a litmus test for businesses and governments alike to show their commitment to serving all stakeholders. With companies vying with each other to receive large amounts of loans and other financial assistance, transparent business conduct will be more crucial now than ever."

FATAL POLICE SHOOTINGS

After Ferguson Police Officer Darren Wilson shot and killed Michael Brown, Jr., an unarmed Black man, in 2014, law enforcement agencies across the United States introduced body camera policies, training methods, and more to reform police use of force.

Despite reforms, fatal police shootings in the United States remain consistent.



SOURCE: *The Washington Post*, June 2020

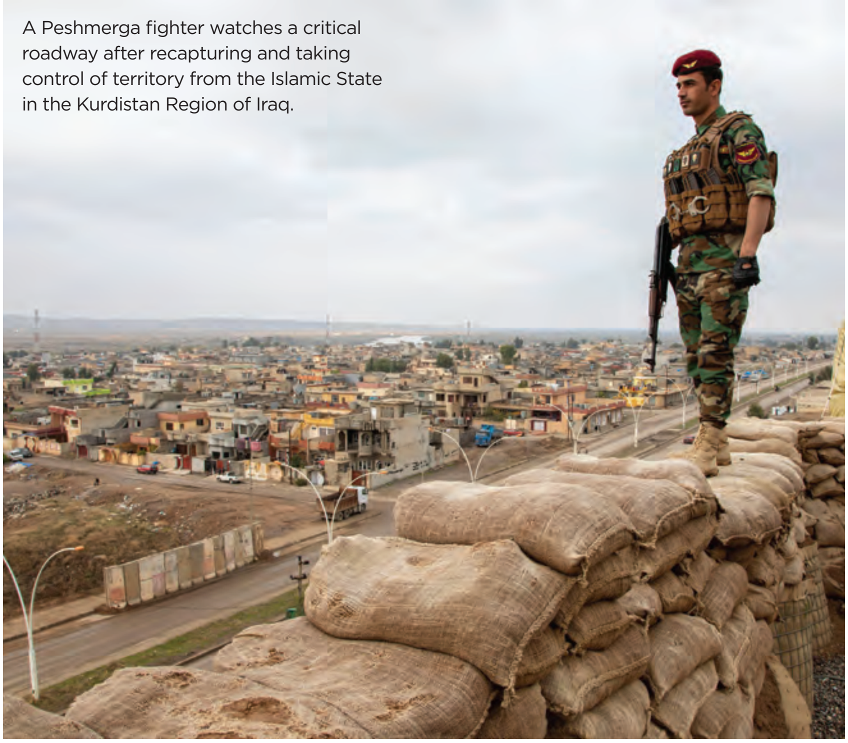
CRACKDOWN ON ART TRAFFICKING

More than 19,000 archaeological artifacts and other artworks were recovered as part of a global operation across 103 countries, resulting in the arrest of 101 suspects and encompassing 300 investigations in a coordinated crackdown, Europol announced in May.

The criminal networks involved handled archaeological goods and art looted from war-torn countries, museums, and archaeological sites. Artifacts seized in global Operation ATHENA II—led by the World Customs Organization and Interpol—included coins, ceramics, historical weapons, paintings, and fossils.

Some highlights of the multinational operation, as touted by Europol, include the recovery of rare pre-Columbian objects—such as a Tumaco gold mask, gold figurines, and ancient jewelry—at Barajas airport in Madrid; the seizure of 2,500 ancient coins following an Argentinian Federal Police Force investigation of a single case of online sale; and the last-minute seizure of 971 cultural objects at Kabul airport by Afghan Customs, just as the objects were about to depart for Turkey.

"Organized crime has many faces," said Catherine de Bolle, Europol executive director, in a press statement. "The trafficking of cultural goods is one of them; it is not a glamorous business run by flamboyant gentlemen forgers, but by international criminal networks. You cannot look at it separately from combatting trafficking in drugs and weapons: we know that the same groups are engaged, because it generates big money. Given that this is a global phenomenon affecting every country on the planet—either as a source, transit, or destination—it is crucial that law enforcement all work together to combat it."



A Peshmerga fighter watches a critical roadway after recapturing and taking control of territory from the Islamic State in the Kurdistan Region of Iraq.

PHOTO BY U.S. ARMY, ALAMY STOCK PHOTO

THE ISIS RESURGENCE

DESPITE THE LOSS OF ITS TERRITORY, THE ISLAMIC STATE MILITANT GROUP STILL POSES A GLOBAL SECURITY THREAT WITH ITS WORLDWIDE REACH. **BY MARK TARALLO**

IN MAY 2020, a video was released that not only received zero rave reviews—it horrified most viewers. The work was produced by the Islamic State's (ISIS) operation in Iraq, and the clear theme running through the video was that ISIS fighters were ramping up terror attacks.

The video's runtime of 49 minutes—long by terror propaganda standards—reflects ISIS's recent surge in claimed attacks across Iraq, according to Daniel Lebowitz, senior analyst at the Terrorism Research and Analysis Consortium (TRAC). "The group's potency is demonstrated by the variety of operations, whether they be improvised explosive devices (IEDs), rocket attacks, or ambushes," Lebowitz explained in a recent TRAC incident report.

The video shows what appear to be assassinations of Iraqi police and militiamen, as well as ISIS snipers operating in broad daylight and armed patrols roaming freely, according to TRAC. In addition, it features other destructive acts that ISIS may turn to more frequently in the future—crop burnings and arson wildfires.

In the summer of 2019, ISIS allegedly tried to extort taxes from farmers and then set fire to the farmers' fields when they refused to pay. The group also took credit for a 2019 series of wildfires in Syria and Iraq. Now, ISIS has been advocating to supporters and sympathizers that arson attacks can be an effective method of jihad.

The terror group has also been encouraging followers to plan more attacks while governments are focused on combating the COVID-19 pandemic. For example, in March 2020 ISIS called on its affiliates in India to conduct attacks as Indian leaders focused on the pandemic, according to researcher Saurav Sarkar writing in *The Diplomat*. (ISIS itself, however, has indicated it takes COVID-19 seriously; in its *al-Naba* newsletter, it recently instructed followers to wash their hands and cover their mouths while sneezing.)

For ISIS, the 2020 resurgence follows a disastrous 2019. Years ago, the group controlled a swath of more than 30,000 square miles in western Syria and eastern Iraq. It originally claimed this territory as its "caliphate" in 2014, and it began exerting a hardline rule over a population of nearly 8 million people, generating billions of dollars in oil revenue and ill-gotten gains from criminal acts like robbery and extortion.

But after 2014, ISIS gradually lost more and more of its territory, and in early 2019 Syrian opposition fighters announced that ISIS had lost the last remaining portion of its land base. Nonetheless, U.S. military officials warned at the time that it was important to maintain an active offensive against ISIS leaders and the spread of their jihadist ideology. Then in October 2019, a U.S.-led operation resulted in the death of ISIS leader Abu Bakr al-Baghdadi in Syria.

In 2020, TRAC is not the only band of experts warning about an ISIS regroup. In March, the United Nations (UN) Analytical Support and Sanctions Monitoring Team, which tracks the global jihadi terror threat, released a report to the UN General Assembly about an ISIS resurgence.

"ISIS has begun to reassert itself in both the Syrian Arab Republic and Iraq, mounting increasingly bold insurgent attacks, calling and planning for the breakout of ISIS fighters in detention facilities," the UN team found. "Freed of the responsibility of defending territory, there was a notable increase in attacks in previously quiet areas held by the government of the Syrian Arab Republic around the country."

The UN team cited a few factors behind its findings. One is that the reduction of U.S. forces in Syria has raised concerns about the ability of current security forces in the country to maintain control of detained ISIS fighters and their family members, a population that exceeds 100,000.

There is also concern about foreign terrorist fighters. The UN team's report cited one assessment that up to two-thirds of the 40,000 aspirants who joined the ISIS caliphate are still alive. "This is expected to aggravate the global threat posed by ISIS, and possibly al Qaeda, for years to come," the team wrote.

Moreover, the report raises concerns about how ISIS-affiliated groups around the world are jumpstarting operations. "In West Africa, the combined efforts of the affiliates are threatening the stability of fragile member states in the region," the team wrote. For example, it cited attacks and arms gathering by the Islamic State West Africa Province (ISWAP) group in the Lake Chad Basin region, near the intersectional border of Nigeria, Chad, and Cameroon.

ISWAP is one of the three most significant terror groups in the Lake Chad Basin, confirms security expert Kabir Adamu, managing director and founder of Beacon Consulting and a former chair of the ASIS International Abuja Chapter in Nigeria. The other two are Boko Haram and a shadowy group sometimes called the Bakoura Faction, Adamu tells *Security Management*.

The activities of these three terror groups are a major factor contributing to the insecurity situation in northeast Nigeria, he explains. "ISWAP continues targeting security forces and civilians with various types of attacks, such as shootings, facility intrusions, abductions, and IED-related attacks, including road planted and body worn as well as vehicle conveyed," Adamu says. The group is also known for destroying and looting civilian properties, he adds.

One emerging trend for ISWAP is the use of long-range 122-mm rockets, Adamu explains. In April, ISWAP asserted in its online magazines and social media platforms that its operatives were conducting rocket attacks, and the group later claimed responsibility for a rocket shooting in northeast Nigeria. Given the long-range capabilities (about 12 miles) and the lack of precision of this weapon system, collateral damage is a significant issue.

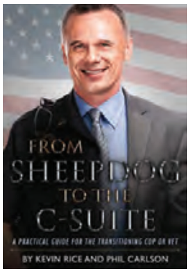
"It represents a risk of collateral targeting for organizations and individuals in near proximity of security forces formations, which are the primary targets of these attacks," Adamu says.

In Europe, "ISIS is actively working to re-establish the capacity to direct complex international operations," the UN team found. ISIS did suffer a setback there in late 2019, when a successful Europol-led mission resulted in the removal of large quantities of ISIS

CAREER TRANSITIONS

BY KEVIN RICE AND PHIL CARLSON.
Book Baby; bookbaby.com; 200 pages; $15.99

TRANSITIONING FROM ONE CAREER to another can lead to high stress and uncertainty, but also to personal discovery for many individuals, including those who have taken an oath to serve and protect their fellow citizens and countries. The focus of *From Sheepdog to the C-Suite: A Practical Guide for the Transitioning Cop or Vet* is to help readers understand the dynamic environment they may face when leaving public service and entering the private sector.


FROM
SHEEPDOG
TO THE
C-SUITE
A PRACTICAL GUIDE FOR THE TRANSITIONING COP OR VET
BY KEVIN RICE AND PHIL CARLSON

Authors Kevin Rice and Phil Carlson address multiple aspects of the process: preparation to exit public service, making the transition, and what to expect when new to the industry. While at times the authors present a pessimistic view of the security industry and private sector in general, they succeed in highlighting real-world situations and circumstances some job applicants face. Great advice is offered in character development, improving knowledge, networking, and other disciplines. The authors show courage in acknowledging that some organizations still acquire talent through personal recommendations from individuals the applicant has previously worked with.

The book is effective in delivering the message to the reader by presenting the information in a personal manner, which mimics the feeling of receiving advice from a longtime friend. Most readers will enjoy reading the last section of the book, which discusses the results of a survey the authors conducted while researching the book. The survey engaged senior-level security leaders across multiple industries and sectors, and its results provide unique insight into what these security professionals are looking for in their future and current staff members.

Absent from this book is practical advice on how to translate skills from public-sector jobs and apply them to private-sector jobs. While transitioning service members and law enforcement will find this book useful, others entering or progressing within the industry will also find value in its message. This book will provide the reader with an advantage over those who have not prepared for their transition. Overall, the book succeeds in its focus, and readers can glean advice they can implement in their own careers to achieve greater levels of success.

REVIEWER: *Danté I. Moriconi, CPP, PCI, PSP, CFE (Certified Fraud Examiner), is physical security manager for L3Harris. He is a member of the ASIS Salt Lake Chapter.*

online propaganda. Still, "the threat of a planned complex attack in Europe, especially by former expert operatives who have the ability to operate independently, is assessed to persist," the UN team found.

In Asia, "groups affiliated with ISIS remain a persistent and growing threat to the region," the team found. For example, in the southern region of the Philippines, several ISIS-affiliated groups have carved out a space for training and operational planning, and they are drawing fighters from Malaysia and Indonesia. Porous maritime borders with visa-free or visa-upon-arrival entry from some countries have helped create a path to the region by foreign terrorist fighters.

Overall, the UN team found that the worldwide threat from ISIS is a significant one—in large part because of the group's resources. The group's financial reserves are estimated between $50 million and $300 million, and the organization continues to attract adherents in many countries.

"ISIS foreign terrorist fighters, adherents, and dependents will continue to pose a terrorist threat over the short-, medium-, and long-term on a scale many times greater than was the case with al Qaeda from 2002 onwards, based on the much greater numbers involved," the UN team found.

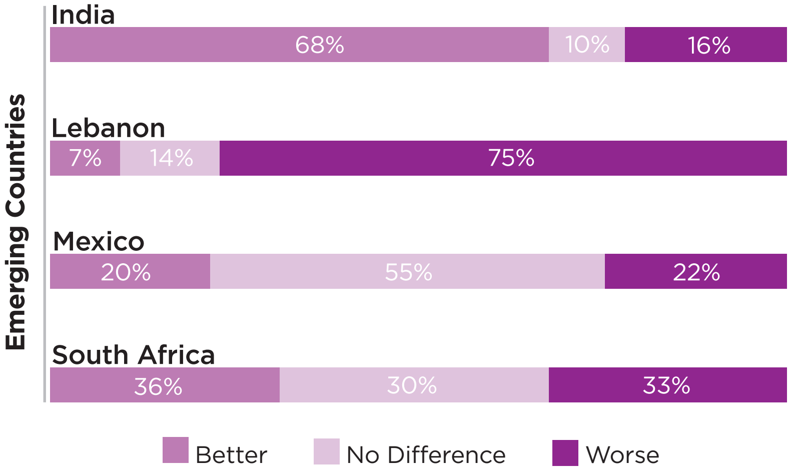
Given this situation, mitigating this threat will take a multi-layered strategy, experts say. A key part of this strategy could be repatriation programs, like one now running in Kazakhstan, that not only accept citizens that left to join ISIS, but also attempt to support and deradicalize them and assist with their reintegration in society.

"Repatriation of these people to their states of origin and nationality will be challenging in the short term," the UN team wrote. "But it holds out the greatest hope of mitigating the longer-term threat."

@ To read the reports cited in this article, see SM Online.

LIVING WITH DIVERSITY

% who say having an increasing number of people of many different races, ethnic groups, and nationalities in their country makes it a ______ place to live.



SOURCE: *Attitudes Toward Diversity in 11 Emerging Economies,* Pew Research Center, June 2020

PHOTO BY iSTOCK

A CENTRAL PERSPECTIVE

WITH MORE THAN 90 BRANCHES ACROSS FOUR U.S. STATES, CITY NATIONAL BANK USES A CENTRALIZED VIDEO AND SURVEILLANCE MANAGEMENT SYSTEM TO MITIGATE LOSS. **BY SARA MOSQUEDA**

DURING THE 1980S AND 1990S, video cassette recorders (VCRs) became a staple in many homes and businesses. But bit by bit, VCRs' reign was overtaken by DVD players and newer technologies that emerged—offering not only the entertainment industry, but also surveillance applications more features and advancements. As the technology was refined and mass-marketed, it became more affordable. So, when City National Bank decided to upgrade its video surveillance system, it looked for technology that could keep up with the changing times.

Roughly 12 years ago, City National Bank experienced a loss incident that emphasized the need for an update. If the bank had been using different technology than VCRs, it may have been able to prevent the loss, says Mary Charles, senior fraud investigator for City National.

Charles, who is both a security professional and a certified fraud examiner, says she knew the bank needed a system that would offer more than just surveillance of individual branches. Operating as localized cells without a central nervous system, the VCR feeds could not be easily accessed by security officers and leaders based at City National's headquarters in Charleston, West Virginia.

Video management was another priority, especially as the bank had approximately 60 branches at the time of the incident and since then has continued to grow. Through new sites and the acquisition of other banks, City National now has more than 90 locations across West Virginia, Kentucky, Ohio, and Virginia.

So 12 years ago, when Verint Systems approached City National and showed their Op-Center and Vid-Center solutions, Charles saw a system that could adapt with both the times and future expansions.

Vid-Center, a video management system, allows a user to watch videos from multiple network video recorders regardless of where those recorders are based. When paired with Op-Center, a video management software, City National branch managers could easily access their respective video feeds while also centralizing all feeds at City National's headquarters. But what sold Charles on the solutions was the ability to save her department an extremely precious resource: time.

Prior to adopting the Verint solutions, Charles had to spend a chunk of her time every week collecting and then combing through 60 branches' individual video feeds just to make sure that all the cameras were functioning properly. But Op-Center would instead send her an email alert if—and when—a camera or other safety solution was faulty. It would even alert her if a camera's view had been moved or altered or if a hard drive was running too hot.

"That was a game changer for me," Charles says. She adds that she knew it would free up time that could be used for her other responsibilities, such as fraud detection. Additionally, early detection of equipment issues would allow for faster maintenance, giving potential bad actors less time to take advantage of a less than ideal situation.

> ***If I'm looking for a suspect and he or she has gone to three or four different branches, I can pull up those different branches at one time instead of doing it one at a time.***

Other features of the centrally managed Op-Center include allowing users, even remote branch managers, to view footage and export images to assist law enforcement, while system managers can determine individual user privileges, update firmware, generate audit reports, and more.

Installing the software was relatively easy, according to Charles, and linking cameras to the central hub is straightforward. For new branches, or ones acquired by City National, IT security technicians link the branches' cameras to Op-Center, identifying individual units by their respective Internet protocol (IP) addresses, and giving Charles and her department secure access to video feeds across the bank's four-state footprint. Essentially, City National expands the system every time it opens or acquires a new branch; the latest expansions occurred in 2018 when two bank companies were acquired, resulting in roughly 17 more branches' video feeds looped into City National's security hub.

City National started off with the basic model when it first integrated the Verint solutions. As the department and satellite branches became more familiar with the system, different components were gradually changed out or upgraded every year. Other updates included switching cameras from analog to IP and replacing old alarm panels wired into a phone line with ones linked to the corporate server to create a line of constant communication. "It has really changed security," Charles says.

The solution also allows Charles to keep tabs on any branch connected to the Vid-Center in real time. Its remote viewing and analysis functions let her notify branch managers of any issues that may arise.

"If someone calls me and there's a live situation going on, I can pull up the camera and see what's going on," Charles says. And if she receives a subpoena for video footage concerning a certain date or event, the feeds are organized and managed so she can easily go back, review the incident in question, and provide the relevant video.

The bank's Op-Center and Vid-Center were scheduled to receive another upgrade in early 2020; however, the coronavirus pandemic and subsequent stay-at-home orders for West Virginia and other states meant delaying the update.

Charles says she looks forward to returning to her office, at which point the upgrade can be installed. The enhancement will allow her to simultaneously pull up and view multiple branch feeds—another time-saving feature.

"If I'm looking for a suspect and he or she has gone to three or four different branches, I can pull up those different branches all at one time instead of doing it one at a time," Charles says.

When she is working on a fraud case, Charles says she anticipates that this latest feature will make the information more readily available. In turn, this will allow her to quickly filter through footage and share relevant information with law enforcement.

FOR MORE INFORMATION, VISIT *VERINT.COM/VIDEOSOLUTIONS.*

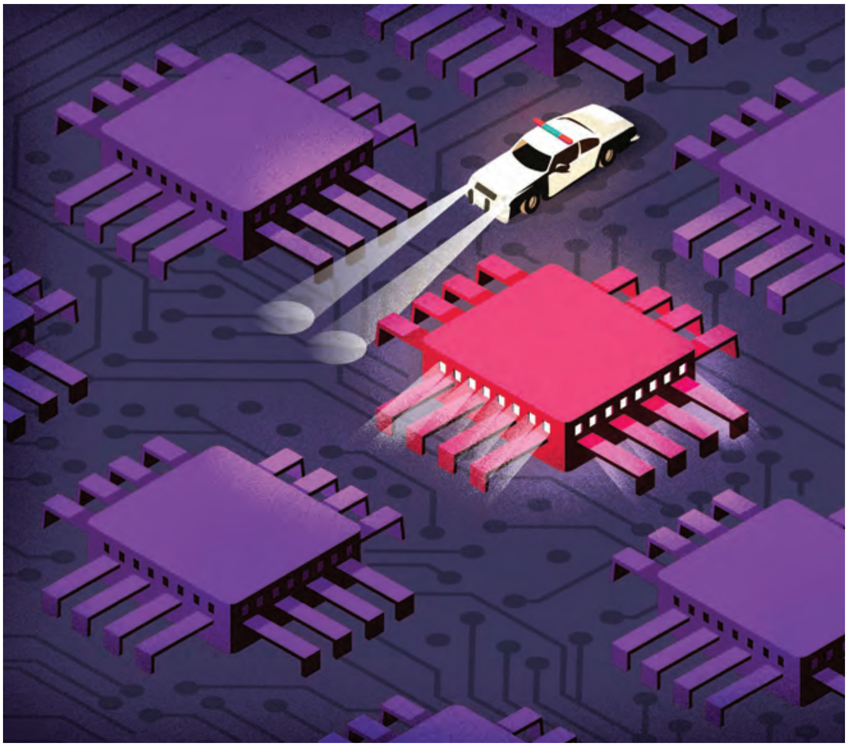


ILLUSTRATION BY RAUL ARIAS

A PATROL PROBLEM

ORGANIZATIONS ARE GETTING BETTER AT PATCH MANAGEMENT, BUT THEY STILL FAIL TO INVEST IN CAPABILITIES TO DETECT AND RESPOND—QUICKLY—TO DATA BREACHES, AN ANNUAL REPORT FINDS.

BY MEGAN GATES

THE FBI CITIZENS ACADEMY is a staple of the Bureau's community building initiative. Held over the course of six to eight weeks in cities throughout the United States, FBI agents educate business, religious, civic, and community leaders about how the Bureau investigates crimes and protects public safety.

When John Loveland, global head of cybersecurity strategy and marketing for Verizon, attended the academy, the agent in charge discussed tactics the FBI uses to detect bombers and provide security at large scale events—such as the Boston Marathon. One common approach is placing police cars and officers near major intersections to monitor traffic and identify suspicious activity.

"There was a question in the course of, 'Are you relying on those metro police officers to detect if there's a truck bomb?'" Loveland says. "The agent's comment was, 'If I have to rely on those guys, I've screwed up.'"

The FBI instead relies on investigative and detection methods that would ideally alert the Bureau to a potential bomber long before he or she went by one of those police officers stationed at a traffic ramp. But this is often not the approach that organizations are taking towards cybersecurity.

"We're spending a lot of time putting cop cars at the entrances to our networks to keep bad guys out, but at the end of the day, the exploits are such that some hackers are going to get through," Loveland says. "Companies have to be spending as much if not more on tech and solutions that help quickly detect when there's an anomaly in the system."

Loveland's assessment is based on findings from the *2020 Verizon Data Breach Incident Report (DBIR),* which found that while containment time for a data breach is down to days or less "discovery in months or more still accounts for over a quarter of breaches."

Now in its 13th year, the report has grown to analyze 32,002 security incidents of 157,525 total incidents from data submitted by 81 contributors from 81 countries. Verizon defines incidents as "security events that compromise the integrity, confidentiality, or availability of an information asset."

The report also includes analysis by industry—broken out into 16 verticals—to help practitioners improve their ability to defend against and mitigate the effects of data breaches (an incident that results in confirmed disclosure of data to an unauthorized party), of which there were a confirmed 3,950 in 2019.

There were a few key themes presented in the data this year. The first was that the use of ransomware continues to grow—representing 20 percent of all malware-related breaches in 2019. Verticals that saw the greater rise in ransomware attacks were against education and state and local governments.

"We saw a trend in that direction that just really caught fire," Loveland adds. "I venture to say that a majority of the tier 1, tier 2 municipalities have faced some form of ransomware attack."

We're spending a lot of time putting cop cars at the entrances to our networks to keep bad guys out.

Ransomware is primarily being introduced to the environment through phishing, which is used to capture user credentials to gain access to Web applications, Loveland says.

This has even greater consequences as the world continues to move towards the cloud and rely on security as a service (SaaS) applications.

"You're expecting [Amazon Web Services] and these platforms to have high level, high grade security to prevent break-ins," Loveland explains. "But a point of vulnerability remains with compromised user credentials. Robust security is possible, but if someone gets ahold of your or my credentials and uses it to access the system—all those defenses are for naught."

And the individuals often behind these breaches are external actors (70 percent) typically associated with organized criminal groups (55 percent of breaches). Most of these breaches were carried out for financial gain (86 percent) and were discovered in days or less (81 percent).

"One thing that gets press attention is nation-state actors looking for intellectual property—that's stolen or used for competitive advantage," Loveland says. "That occurs in manufacturing and the public sector, but by and large these breaches are financial in nature."

Loveland also explains that breaches are perpetrated by insiders, but that does not always mean the insider is acting maliciously. Many of these breaches are the result of errors or misconfigurations in systems that inadvertently cause a data breach.

"...in spite of what you may have heard through the grapevine, external attackers are considerably more common in our data than are internal attackers, and always have been," according to the report. "This is actually an intuitive finding, as regardless of how many people there may be in a given organization, there are always more people outside it. Nevertheless, it is a widely held opinion that insiders are the biggest threat to an organization's security, but one that we believe to be erroneous. Admittedly, there is a distinct rise in internal actors in the data set these past few years, but that is more likely to be an artifact of increased reporting of internal errors rather than evidence of actual malice from internal actors."

The report's authors saw this most frequently in the healthcare vertical, where internal actors were responsible for approximately 50 percent of breaches. This is because they are working in a "fast-paced environment where a huge amount of work must be done and is also facilitated by paper," Loveland says. "They often don't have controls that are up to snuff—leaving lots of room for errors."

Errors have always been common in industries with mandatory reporting requirements—like public administration and healthcare—but are now rising in other industries, too.

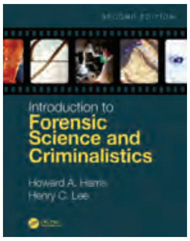
"The fact that we now see error becoming more apparent in other industries could mean we are getting better at admitting our mistakes rather than trying to simply sweep them under the rug," according to the report. "Of course, it could also mean that since so many of them are caught by security researchers and third parties, the victims have no choice but to utter 'mea culpa.'"

In fact, security researchers were the individuals most likely to alert organizations of a data breach—notifying organi-

FORENSIC SCIENCE

BY HOWARD A. HARRIS AND HENRY C. LEE. CRC Press; crcpress.com; 420 pages; $89.95.

THE TOPIC of forensic science and criminalistics can be of interest to the security profession in the identification and protection of evidence in an investigation, but it is not a function that would normally be the responsibility of a security professional.



The second edition of *Introduction to Forensic Science and Criminalistics* is of value to students of or those engaged in the collection and analysis of evidence in a criminal case.

The authors of the book are leaders in their profession and offer many years of experience, sharing vast original content and knowledge within the publication. As a criminalistics publication it provides an advanced level of information that is current and valuable. The writing style is organized, concise, and easy to read. The chapters follow a logical sequence covering the topics within the book, including physical evidence, crime scene processing, questioned documents, digital evidence, biological evidence, explosives, and drugs, among other things.

Color photographs, charts, and lists within the publication provide excellent visual context to the book, supporting and enhancing the text. The book provides an abundance of references to back up its data and for future reading. The in-depth index allows for easy retrieval and review of relevant information.

Overall, this is an excellent book for its intended audience. It would be of value to those in the security profession who seek to expand their knowledge of this scientific discipline and to have the publication as a professional reference.

REVIEWER: *Daniel Benny, CPP, PCI, holds a PhD in Criminal Justice and is a tenured associate professor in intelligence and security studies at Embry-Riddle Aeronautical University Worldwide Campus. He is the author of seven textbooks on security matters and has been a member of ASIS International since 1976.*

zations roughly 50 percent of the time, six times higher than in 2018. Less than 10 percent of breaches were reported by internal employees.

This demonstrates the gap that continues to exist in organizations' ability to detect when they have experienced a breach and that the focus on perimeter protection—instead of detection and response—is misguided.

External attackers are considerably more common in our data than are internal attackers.

For instance, organizations should be looking to enhance their detection and response capabilities by creating more points to monitor movement through their network and on devices. These measures are also imperative given the rise of remote work in response to the coronavirus pandemic.

"How are companies extending the security fabric outside their four walls?" Loveland asks. "How do you install that same behavior and vigilance at home that you have in the office?"

One positive finding from the data, Loveland adds, is that there has been a steady decline in vulnerability exploits being used to compromise organizations. A common example of this tactic is the Equifax breach, where a Web application was compromised because the company failed to patch a known security flaw.

"We're seeing patching and patch management start to have an impact in reducing some of the vulnerability exploits and also reducing things like Trojans," Loveland says. "Hygiene is on the increase; it's helping reduce those traditional attacks." ■

@ To read the Verizon *DBIR,* visit SM Online.

WHERE IN THE WORLD DID THE MOST BREACHES OCCUR?

The 13th edition of the *Verizon Data Breach Incident Report,* published in 2020 on data collected from 2019, identified a total of 157,525 security incidents around the world—32,002 of which met Verizon's quality criteria for analysis.

North America led the field with 18,648; followed by Europe, Middle East, and Africa with 4,209; Asia and the Pacific with 4,055; and Latin America and the Caribbean with 87. The report said 5,003 incidents were reported, but they occurred in unknown locations.

One reason North America may have the highest number of incidents is because of its data reporting standards for industries, including healthcare and public administration.

"Therefore, the number of incidents and breaches are likely to be higher than in areas with less stringent disclosure requirements," according to the report. "Also, it must be admitted that while this report is becoming increasingly global in scope, many of our contributors are located in and are primarily concerned with North American organizations."

North American organizations saw a high number of financially motivated attacks against Web application infrastructure, leveraging stolen credentials obtained through social engineering attacks. Europe, the Middle East, and Africa were often targeted by attackers combining hacking techniques that leveraged stolen credentials or known vulnerabilities. The Asia and Pacific region saw a high number of financially motivated actors targeting their systems.

NEW!
The ASIS Certified Protection Professional (CPP®) Study Manual
ASIS INTERNATIONAL
ASIS

CUTTING EDGE

The quarterly supplement from *Security Management* examines technological solutions to security challenges. *Security Technology* features in-depth articles about revolutionary technologies, case studies, and thought leadership pieces from industry experts.

SECURITY TECHNOLOGY

VISITOR MANAGEMENT ENHANCES SAFETY
System providers are being proactive in answering the call to help screen visitors during the COVID-19 pandemic. **p03**

JOHNSON CONTROLS ENHANCES THE VIEW
Gateway Arch National Park adopts a video management solution to provide oversight of its expanded footprint. **p04**

DESIGN SOLUTIONS WITH PRIVACY IN MIND
Technology created with a privacy focus provides tools to restrict access while protecting data. **p10**

FACIAL RECOGNITION NEEDS TO BE REGULATED
Developers and implementers need guidance to create ethical, responsible solutions that benefit society. **p11**

A SUPPLEMENT OF *SECURITY MANAGEMENT*

JUNE 2020

HERE'S LOOKING AT YOU

Regulations and public expectations are changing the way security practitioners address privacy concerns about technology solutions. **p06**

Photo illustration by Security Technology; iStock

Watch for it bundled with
September's *Security Management.*

SECURITY MANAGEMENT | ASIS INTERNATIONAL

COVER STORY | BY CLAIRE MEYER

As in-person classes resume, pandemic-triggered stressors may take their toll on student behavior and security's response.

GRACE PERIOD

ILLUSTRATION BY STEPHANIE DALTON COWAN

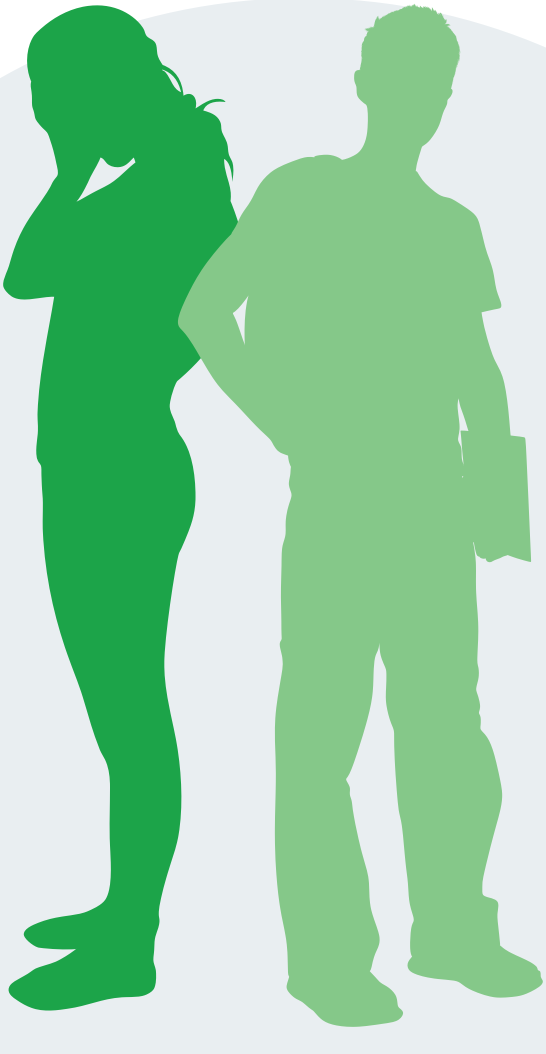
Students around the world learned a harsh lesson in 2020: pandemics can have devastating impacts on lives, economies, and schools. As a result of the coronavirus pandemic, schools closed, academic terms were truncated, routines were broken, and uncertainty and anxiety permeated students' home and social lives. Many school systems considered how best to reopen and weighed physical health and safety measures, but school psychology and security experts cautioned not to discount students' state of mind.

Most teachers and school officials acknowledge there is a typical readjustment and relearning period for students after any break—whether it's a three-month summer vacation, a two-week holiday, or even a snow day. The first few weeks of term are often spent reviewing lessons from the previous year.

However, the series of events related to the COVID-19 pandemic are decidedly different. Schools had to shift gears quickly—often with limited resources—to prepare for virtual learning instead of classroom education. In the United States, school buses were reconfigured to deliver school lunches or Wi-Fi to students at home. Academic performance was frequently judged on a pass–fail system, and students were isolated from their friends, peers, and role models at developmentally critical times.

Students are also at additional risk during the pandemic due to potential parental unemployment, food or housing uncertainty, financial stresses, or illness or death in the family, says Dr. Franci Crepeau-Hobson, an associate professor and director of clinical training at the University of Colorado Denver School of Psychology. Crepeau-Hobson is also cochair of the National Association of School Psychologists' School Safety and Crisis Response Committee.

"Folks who were already stable, had some resiliencies, and had some really strong support systems are going to weather this adequately well," she says. "But those kids who were already vulnerable are the ones we're going to have to be the most concerned about, whether that was because of a preexisting mental health challenge, a disability, or what was going on at home."



Thirty-two percent of California students in grades 5-12 who were not receiving mental health services felt they may need them during and after the pandemic, according to a survey by the American Civil Liberties Union (ACLU) of Southern California in late April 2020.

Before COVID-19, 65 percent of students rated their mental wellness—defined for the survey as the ability to cope with the normal stresses of life and work productively—at 7 or above on a 10-point scale. But at the end of April, less than 40 percent of students rated their mental wellness at the same level; 23 percent of students rated their mental wellness at 3 or lower, signaling a need for action and assistance.

The survey noted that students frequently described their mental state as bored, lonely, overwhelmed, and anxious, particularly noting concerns about schoolwork, the wellbeing of their families, general uncertainty, and missing out on typical school experiences.

"Students have been so very isolated from their peers at such important social development periods, and they have been disconnected from the larger community, while parents are struggling," says Michele Gay, cofounder and executive director of Safe and Sound Schools. "No matter how functional a family is or how well suited it is to withstand this type of challenge, parents have been distracted. If they're lucky, they are able to work from home, but it's been a challenge to support their kids, to keep them on track with academics, to deal with their frustrations, anxieties, and depression, all while handling their own responsibilities within the family. Kids have been sponging these effects up.

"So, when we are able to reconnect—hopefully in the fall—we know schools are not going to be the same. We know kids will be coming back with a lot of negative experiences," she adds. "They will have felt the effects of stress on the family—financial stress, the day-to-day stress of being locked in together. There will be academic regression, and we know to expect social–emotional regression. Oftentimes these things manifest in negative behaviors—bullying, being grumpy, disconnected, or oppositional. School is going to be more about reconnecting and developing a supportive culture and learning how to communicate again."

There is also the uncertainty of not knowing what the fall will look like because "we don't have an expiration date on COVID-19," Crepeau-Hobson says. To cope with this uncertainty, it is helpful for school districts to remind personnel and educators about existing processes for reporting warning signs that a student is struggling, as well as refreshing procedures around school security, student support, hygiene, and education.

Security's role in this process might seem invisible to most stakeholders in the community, Gay says, "but we know that the school environment has a tremendous impact on the sense of safety, the feeling of safety. The underlying foundational feeling of safety is even more important than ever, especially when emotions are high and students and staff come back to school with anxiety. To simply be able to show that the space is as safe as it possibly can be, that supports the sort of social–emotional environment that we to build."

Stress and Student Behavior

Once the realities of the pandemic started to set in among American school districts, Safe and Sound Schools almost immediately started getting reports of emotional effects on students, educators, and administrators.

As schools reopen, school officials need to "be prepared for the emotions," Gay says. "People can be very unpredictable when experiencing unknown emotion. As excited as we all are about the prospect about returning to school, it's not going to be the school that we left. We're going to return with different experiences. Security and safety personnel, administrators, and teachers all need to be prepared for that. Be on the lookout for warning signals or signs that someone might need support or help—students, parents, or staff members—and have prepared safe spaces. People might need a safe, quiet place to retreat, regroup, or have a conversation with a counselor or peer."

In addition, be prepared for challenges to school officials' authority. In the early stages of the pandemic, schools were bombarded with information and guidance—much of it nebulous or conflicting. Students were paying close attention to the misapplication of information, and they may be distrustful of new guidance once schools reopen, says Paul Timm, PSP, president of Facility Engineering Associates, P.C., and a member of the ASIS International School Safety and Security Council. Some students might even be more well-informed than school officials about the virus, and they might walk into the building and question new measures in a show of defiance or disagreement, he says.

Students will wonder what to expect when coming back to school, and it is likely that school staff will experience a period of students' testing the limits of new measures, Crepeau-Hobson adds.

Upon their return to school, students might be emotionally shut down or worried, or they could become disruptive and aggressive. In response, schools need to provide tangible signs of how safe the school is, both physically and psychologically, and create a caring and connected environment, she says. This might involve performing some tasks—like cleaning and sanitizing—during the school day to ensure that students see the precautions being taken, on top of measures such as physical distancing, Plexiglas barriers in lunch lines, or staggered school schedules.

At the end of this honeymoon period, Crepeau-Hobson says, if adults have done their jobs, students will feel safer and act out less.

A united front will go a long way to heading off these behavioral challenges. When the school district speaks with one voice and communicates openly about new measures and the rationale behind them, it can help diffuse any student–faculty tension over health and safety measures.

When disruption does occur, however, make sure school discipline is woven in with support—both at the academic and social–emotional levels, she adds.

Physical and Psychological Safety

Students are processing the effects of the pandemic in a number of different ways, Crepeau-Hobson says, but the warning signs of a child in trouble remain largely the same: sudden changes in personality or behavior, withdrawal, aggression, changes in academic levels, indications of lethargy, and self-harm.

Children with the tendency to externalize their emotions might exhibit a constant state of alarm, requiring additional reassurance.

"All this uncertainty is really tough for people—we don't feel safe because we don't know what's going to happen. We're walking around in this constant state of alarm where our brains are communicating 'I'm not safe, I'm not safe,' so we're kind of on edge anyway," she says. "Some folks are better at managing that and regulating themselves, but kids often need help. You may see more dysregulated kids, which means they can't manage their own behavior and their own emotions."

In response, faculty can be trained to watch for warning signs and changes in behavior and learn how to respond. It's key not to jump to conclusions—if a student acts out in the classroom, for example, he or she might simply be having trouble readjusting to school routines due to their anxiety. At the beginning of the year, Crepeau-Hobson recommends cutting students some slack.

Additionally, provide some means for students to regulate their emotions. This could include modifying academic expectations so the first few weeks of school have less pressure to achieve, restructuring the school day to add more breaks, or adding calming activity sessions between classes.

It's also fundamental that adults themselves are emotionally regulated. "If you have dysregulated adults, you are not going to have any regulated kids; they're going to be a mess," she adds. "So, we have to make sure that adults are walking in feeling safe and supportive, and that they know what to do, because that's empowering."

School security personnel should also partner with social–emotional leaders such as school counselors and psychologists, Timm notes.

"This is a collaborative effort, and we should be relying on their expertise more than ever," he says.

Pandemic-related stress is likely to heavily affect students with mental health challenges, says Guy Grace, director of security and emergency planning at Littleton Public Schools in Colorado. Over the remote learning period at the end of the school year, Grace and his security team performed welfare checks and virtual check-ins with students who missed virtual classes or exhibited signs of stress.

"Suicide risk and mental health risk have not decreased at all; they may have increased. We wanted to make sure we didn't let those kids fall through the cracks," he says.

Schools play a pivotal role in getting at-risk students help, even if stressors originate from outside sources, says Dr. Scott Poland, co-director of the Suicide and Violence Prevention Office at Nova Southeastern University. According to the National Institute of Mental Health, suicide is now the second-leading cause of death for individuals between the ages of 10 and 34 in the United States. In 2017, 517 children aged 10-14 died by suicide in the United States; among 15- to 24-year-olds, 6,252 died by suicide.

School districts can set aside a 45-minute briefing for staff to review mental health crisis warning signs and procedures for how to refer a student to get help. Giving the school counselor time to address the faculty about how to escalate the issue can clarify both warning signs and next steps for school staff. It will also increase awareness of mental health and suicide risks in schools, particularly when considering the additional stressors introduced by the pandemic, Poland says.

When classes resume in person, however, schools are likely to feel the financial burden from COVID-19 mitigation measures, which could take a toll on school safety initiatives like mental health or school violence prevention, Grace warns. It will be a difficult balancing act in the near-term to respond to the immediate threat of COVID-19 without losing sight of long-term, ongoing risks.

In addition, he says it is security's role to ensure students are comfortable with the new health and safety measures put in place. After the shooting at Columbine High School in 1999, schools across the United States introduced hardening measures like metal detectors or high fences, which was frightening, especially to younger students. If students are met at the door by a medical professional during the pandemic, it could scare them away from returning to school, Grace says.

"School systems can't avoid the responsibility of relieving fear and anxiety as much as possible when students come back," he says. "We have to be careful about how we do this. We have to put the best practices in that will protect kids and staff members, but also help ensure that this is a place teachers want to come to teach, students want to learn, and parents won't worry about their kids in school."

Education around COVID-19 mitigation measures can be tailored to students' developmental levels to ensure mitigation is not compounding existing anxiety, Grace adds. For elementary school children, schools can emphasize handwashing, hygiene, and physical distancing, and keep other mitigation methods in the background—similar to what school security personnel do for severe weather drills and education. But at the middle and high school levels, students can be more empowered to take care of themselves and others.

"It's all about empowering students and staff on how they can deal with emergencies," Grace says. "Education goes a long way in mitigating the fear and the angst that people are going to have on a day-to-day basis. Educational empowerment is critical to maintaining a functional school environment."

"Educational empowerment is critical to maintaining a functional school environment."

Caring for the Caregivers

Students are far from the only ones under significant pandemic-triggered strain. School budgets are stretched, educators have grappled with the shift to virtual learning, and school personnel have been forced to cope with personal loss, financial uncertainty, and emotional stress.

In this respect, Dr. Scott Poland, co-director of the Suicide and Violence Prevention Office at Nova Southeastern University, recommends following the advice of airplane safety: Put your own oxygen mask on first.

"Kids are going to look to the adults in their life to see how upset to be about something, and understandably a lot of adults are fearful and anxious," he says.

Poland suggests adults remember the simple mnemonic CALM: Control, Availability, Listening, Managing.

In the midst of uncertainty and change, remember what you can control: your responses and following recommended medical guidelines. Second, be available for children. "Most kids just need an opportunity to talk about their experience," Poland says.

Third, listen closely to what students say, and when possible, limit media consumption to avoid overstimulation and stress. Finally, manage your reactions and emotions as best you can because children are monitoring actions as much as words for cues on how to respond to stress.

Using this model, school security personnel can serve as role models for students, intervening in emerging conflicts and demonstrating appropriate behavior.

Security personnel are "supposed to be a resource, they're supposed to be a symbol of safety, they're supposed to take active steps to keep kids safe," says Dr. Franci Crepeau-Hobson, an associate professor and director of clinical training at the University of Colorado Denver School of Psychology.

While many school stakeholders primarily associate security with physical safety, they are key to psychological safety as well, she adds. "By being a connected member of the community, by being out in the hallways and lunchroom and on the playgrounds, they are visible, connected, and seen as a resource for kids, to let them know they're okay."

Communication

Students will look to parents and teachers to see how to react to stressors, Poland says, and nothing undercuts a safety message quite like politics.

In presenting a united front around school safety measures, teachers and faculty should strive to keep political opinions, emotional responses, and personal views out of the way. Poland recommends displaying confidence in the people making decisions—especially the scientists and subject matter experts searching for solutions—and collecting input from students and staff on how to make existing school-specific measures even better.

"The wisest decisions are made by a group of people," Poland says.

At Milton Hershey School, a pre-K through 12th grade residential school for underprivileged children in Pennsylvania, collaborative communication has been essential in pandemic response so far. Of the school's 2,200 students, 500 remained on campus during the initial months of the pandemic in the United States. This required the reconfiguration of student housing to focus on social distancing and virtual learning, and as of *Security Management*'s press time, the school is finalizing a system to safely reintroduce students returning to campus.

"Communication was one of the key things right out of the gate," says Rick Gilbert, senior director of campus safety for the Milton Hershey School. "A lot of schools, like us, felt like we had some good pandemic plans in place, but not to this magnitude…We always revisit what kind of communications can we get out there and how quickly can we get it out without causing a panic, and providing accurate information at the same time. Given that information was evolving so quickly, within a matter of 48 hours, things would change all over again."

In response to the rapidly shifting health crisis, the school established a COVID-19 taskforce under the incident response function. Through that taskforce, the communications team collected input and content to share with parents, sponsors, staff, and leadership in a cohesive message.

When students' parents or sponsors had specific questions, they could send them through a dedicated email address. Daily emails with relevant updates were sent out to staff, leadership, and parents or sponsors respectively, and more timely information was shared via mass notification tools, Gilbert says.

Communication with students is also vital, he adds. Milton Hershey's family resources department has established

NOT ALL THREATS ARE THIS OBVIOUS
With the rise of security threats on campuses, put your trust in an American made product that you can rely on to keep your students safe.
PD 6500i
PINPOINT
DETECTION
PD 6500i Walk-Through Metal Detector
GARRETT®
METAL DETECTORS
MADE IN THE USA
ISO 9001 CERTIFIED

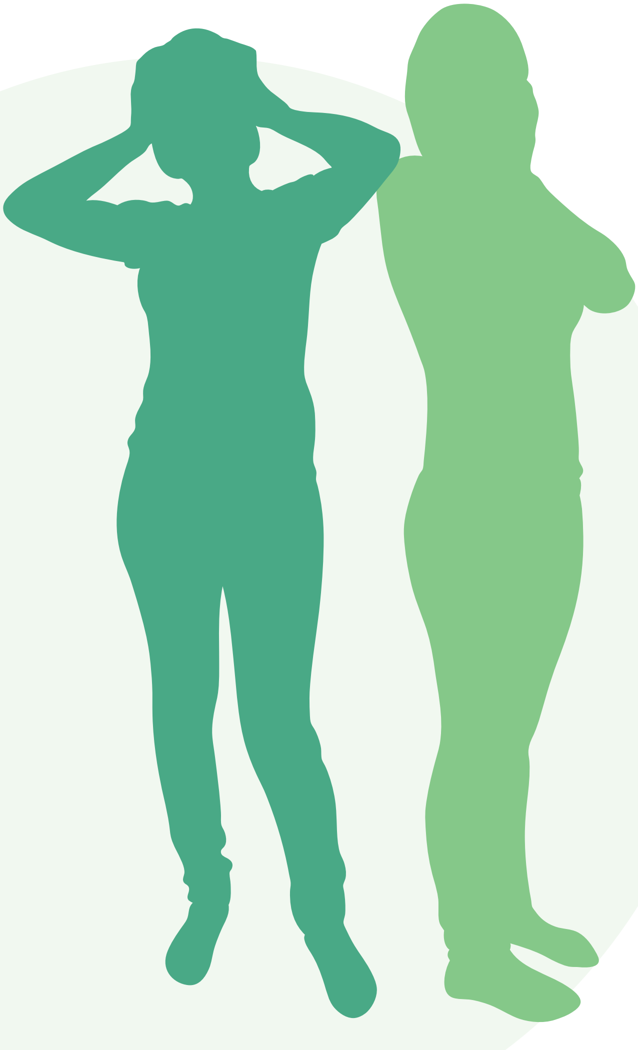
rapport with students and their families to keep in touch and address challenges while students are off-campus. The counseling department is available to help address any student anxiety or angst, either remotely via teleconferencing tools or on campus.

Campus safety is tasked with how to keep COVID-19 mitigation efforts, such as physical distancing measures, in line with existing security.

"I know we will get called upon to enforce some of that," Gilbert says. "It's critical for our folks to understand that our students are coming in with lots of pressure and anxiety. We're not here to crack down. They're not in trouble. They're kids—this is a challenge for them as they see their friends and try to interact. It's going to be critical for us to educate our students on why we're doing this, but we're not looking to come down and enforce what that social distancing looks like. We want to explain that this is for their health and for their classmates' health."

Depending on how the new measures are treated, heavy-handed enforcement could quickly escalate into confrontation, Gilbert warns. "The situation's already tense enough without us raising the anxiety level."

"Empathy can build bridges."



With residential students, campus safety staff already has an established relationship with students and can de-escalate conflict more effectively. At initial signs of defiance or misbehavior, security personnel can talk with the student, and after a few quick questions they learn why that behavior shifted.

"Their routine has completely changed, and they have learned to grow and understand that this is the new norm, and we're all trying to figure this out," according to Gilbert.

"Take an extra two or three seconds to explain the why," Gilbert says. "Our students are very resilient, and I think sometimes we underestimate them. Sometimes they just want to be part of the process."

Students have a lot of insights to bring to the table when developing, adjusting, and deploying new safety measures, Timm says. School districts can bring students into briefings about security systems and new safety measures, he advises.

In addition, districts can recruit student subject matter experts to teach school personnel about emerging technology (learning how to navigate the latest social media like TikTok can help schools respond to digital bullying or threats and help students adjust faster, Timm says) or challenges within the student body.

These sort of short training sessions—whether a three-minute briefing on new video surveillance coverage, a social media primer, or an open discussion on how new COVID-19 mitigation measures are working—can have long-term effects on program buy-in and participation.

"School is all a preparation for vocations and learning and becoming contributing citizens. This is the best time ever to bring students in and get their feet wet in leadership roles," Timm explains.

In the midst of widespread uncertainty during the pandemic, tapping students for these briefings can also empower them and help them regain some control and confidence.

To connect further, Timm recommends being frank and open with students about challenges and concerns that administrators, faculty, and educators have had during the pandemic, whether that's expressing regret over missing out on a baseball season or acknowledging uncertainty about what comes next.

"As much as we want a united front, and we want to speak with confidence about our decisions, I do think there's a part of us that has to be transparent," according to Timm. "If adults and administrators are able to be relationally transparent—just letting kids know that we're in the same boat—I think that's going to cause there to be some camaraderie that we've missed out on until now...Empathy can build bridges." ▨

CLAIRE MEYER IS MANAGING EDITOR FOR *SECURITY MANAGEMENT.* CONNECT WITH HER ON LINKEDIN OR EMAIL HER AT *CLAIRE.MEYER@ASISONLINE.ORG.*

PROTECTION OF ASSETS
SECURITY MANAGEMENT
PHYSICAL SECURITY
INFORMATION SECURITY
CRISIS MANAGEMENT
INVESTIGATIONS
LEGAL ISSUES
APPLICATIONS
PROTECTION OF ASSETS
SECURITY OFFICER OPERATIONS
ASIS

In the Dark

Industrial control systems have traditionally been kept isolated with limited remote network access. But that's changing—introducing new and potentially damaging vulnerabilities.

Essential personnel have made drastic changes to the way they are working in response to the coronavirus pandemic—including electric grid operators.

In an unprecedented step, the New York Independent System Operator (NYISO)—an independent organization charged with managing the state's electric marketplace—announced on 31 March 2020 that it would sequester a group of its control room operators and support staff to protect their health and safety and maintain grid reliability as COVID-19 cases skyrocketed in New York state.

Thirty-seven people—31 grid operators, two managers, two facilities staff, and two café workers—volunteered to join the sequestration program at two NYISO sites outside of Albany, New York. They would work 12-hour shifts and live in separate trailers for the duration of the sequestration—a workflow that was established to minimize cross-contamination.

"Our primary job is to keep the power flowing in New York," NYISO said in a statement. "Operators are on the front lines, making sure that the amount of power being generated always equals the amount of demand from the state's nearly 20 million residents and businesses. To do that, seven operators work per shift, monitoring dozens of digital displays and directing power generators and distributors to keep energy transmission in balance."

Such steps were necessary to keep NYISO operational because much of the equipment that is used to manage, control, and distribute

ILLUSTRATION BY EVA VÁZQUEZ

electrical power is not connected to a network that can be accessed remotely. This is a control mechanism designed to limit exposure to a cyberattack that could cause a power failure.

But with increasing technological capabilities and the need to access worksites remotely—such as during a pandemic—more utility operators are looking at connecting their operational equipment to the Internet, said Tim Conway, technical director of industrial control system (ICS) and Supervisory Control and Data Acquisition (SCADA) programs at the SANS Institute, in a virtual conference on ICS security earlier this year.

"Critical infrastructure is adding remote connection at an alarming rate," he added. "I don't know if we're going to see this go back down after COVID-19...but we need to improve detection capability if that's the case."

This is because ever since the attacks on Ukraine's electrical grid that shut off power in 2015, threat actors have been increasingly focused on targeting critical infrastructure and the systems used to support its operation. North America is an especially lucrative target, and recent analysis finds that regulators may not fully understand the scope of a massive power outage caused by a cyberattack.

The Landscape

ICS is a term used to describe control systems and their instrumentation, which can include devices, systems, networks, and controls that operate or automate industrial processes. These

These systems are an important component of critical infrastructure, such as manufacturing, transportation, energy, and water treatment.

One type of ICS is a SCADA system, which is used to acquire and transmit data and is often integrated with a human interface to provide centralized monitoring and control for process inputs and outputs, according to multinational cybersecurity and defense company Trend Micro.

"The primary purpose of using SCADA is for long distance monitoring and control of field sites through a centralized control system," Trend Micro explained in a blog post. "In lieu of workers having to travel long distances to perform tasks or gather data, a SCADA system is able to automate this task. Field devices control local operations such as opening or closing of valves and breakers, collecting data from the sensor systems, and monitoring the local environment for alarm conditions."

In 2015 and 2016, Russian-backed hackers used cyber tactics to target Ukraine's electric grid and shut portions of it down during the winter—wreaking havoc and causing authorities around the world to bolster their grid security.

Prior to those attacks, the U.S. Government Accountability Office (GAO) placed the protection of critical cyber infrastructure—including the electric grid—on its High Risk List in 2003. In 2018, Congress asked the GAO to audit the cybersecurity of the U.S. power grid, which is interconnected with Canada's and a small portion of Mexico's.

In its research, conducted over the course of a year and published in August 2019, the GAO found that the electric grid is increasingly vulnerable to cyberattacks—especially those involving any ICS that supports grid operations. Increasing adoption of consumer Internet of Things (IoT) devices and the use of the global positioning system to synchronize grid operations were also contributing to the growing vulnerability of the grid.

Critical infrastructure is adding remote connection at an alarming rate.

"Compounding the risk associated with the increased attack surface, many legacy industrial control systems were not designed with cybersecurity protections because they were not intended to be connected to networks, such as the Internet," the GAO explained. "For example, many legacy devices are not able to authenticate commands to ensure that they have been sent from a valid user and may not be capable of running modern encryption protocols. In addition, some legacy devices do not have the capability to log commands sent to the devices, making it more difficult to detect malicious activity."

The GAO also found that grid owners and operators may not be able to identify ICS vulnerabilities in a timely manner because conventional IT vulnerability scanning could disable or shut down energy delivery systems. And for those who do identify vulnerabilities, they may not be able to quickly address them because of high availability requirements needed to support grid operations.

"These devices typically need to be taken offline to apply patches to fix cybersecurity vulnerabilities," the GAO added. "In addition, grid owners and operators need to rigorously test the patches before applying them. Security patches are typically tested by vendors, but they can degrade or alter the functionality of ICS, which can have serious consequences for grid operations."

The GAO also found that the supply chain for ICS could also introduce vulnerabilities that make operators more vulnerable to cyberattacks.

"For example, there is a potential for manufacturers and developers to—wittingly or unwittingly—include unauthorized code or malware in industrial control system devices and systems that provides a back door into the equipment or that allows the program to 'call home' once installed," the GAO explained.

Most concerning, however, was the finding that despite federal assessments indicating cyberattacks could cause widespread power outages in the United States, the government lacked an understanding of what the ramifications of such an incident would be.

"We thought federal assessments of the impact had limitations," says Frank Rusco, director of GAO's Natural Resources and Environment Team and coauthor of the report. "In short, assessments didn't always cover the various cyberattack scenarios that should be considered—such as techniques or coordinated attacks on multiple sites at one time. Some of the assessments did not cover as wide a geographic scale as would have been helpful."

For instance, the assessments did not address the ramifications of a widespread power outage that lasted for a long period of time—as opposed to a storm where the grid was damaged but able to resume operations quickly.

Additionally, one of the three assessments that the U.S. Department of Energy (DOE) was relying on covered the Western Interconnection, which extends from western Canada south to Baja California in Mexico, and east to the Great Plains of the United States, but was based on a reduced model of the electric grid from 1980.

"If you're not modeling what's possible in terms of what could happen, but you're also not looking at the system as it is today and how reliant we are on it…you're going to miss it because you haven't modeled what is actually possible," Rusco says, adding that he is not sure why the U.S. Department of Energy (DOE) was relying on that particular assessment. The DOE did not return request for comment on this article.

The GAO's analysis also found that while the Federal Energy Regulatory Commission (FERC), which regulates the interstate transmission of electricity, natural gas, and oil, has approved mandatory grid cybersecurity standards, it does not ensure that those standards address the National Institute of Standards and Technology (NIST) Cybersecurity Framework. The GAO also highlighted that FERC has not considered the potential risk of a coordinated cyberattack on geographically distributed targets.

"Such an attack could target, for example, a combination of geographically dispersed systems that each fall below the threshold for complying with the full set of standards," the GAO said. "Responding to such an attack could be more difficult than to a localized event since resources may be geographically distributed rather than concentrated in the same area. Without information on the risk of such an attack, FERC does not have assurance that its approved threshold for mandatory compliance adequately responds to that risk."

Actors and Methods

In its *2019 Year in Review: The ICS Landscape,* Dragos—a security firm that specializes in ICS protection—found that despite no reported destructive attacks, the "amount of activity targeting ICS increased significantly in 2019."

The report detailed 11 activity groups that are targeting ICS entities around the world, with an increased focus on ICS organizations in critical infrastructure across the United States and the Asia-Pacific regions.

Dragos assessed that there will likely be an increase in cybersecurity activity

A Flaw in the System

Experts and researchers have raised concerns over the past several years about the security of Supervisory Control and Data Acquisition (SCADA) programs—a type of industrial control system (ICS).

In summer 2020, cybersecurity firm Trustwave published a new vulnerability report by Seok Min Lim on two exploits that could be used to target Schneider Electric's Programmer Logic Controller (PLC) software and hardware. PLCs are flexible pieces of hardware used in SCADA programs and operational technology for utilities. One of the exploits was an expansion of a discovery researchers originally made in 2017, but the other was new, says Karl Sigler, senior security research manager for Trustwave, who oversees the research team Lim is on.

The first vulnerability allowed researchers to "intercept, manipulate, and re-transmit control plane commands between the engineering software to the PLC," according to Trustwave's report. "The impact is that a malicious actor can start and stop the PLC remotely without authentication."

The second vulnerability found that free software provided by Schneider—SoMachine Basic—to program and control a PLC did not perform "adequate checks on critical values used in the communications with the PLC," Trustwave said. "The vulnerability can potentially be used to send manipulated packets to the PLC, without the software being aware of the manipulation."

Trustwave reported the vulnerabilities to Schneider, which has since released patches for them. But the exploits show how these programs and systems are increasingly vulnerable to cyberattacks because of flaws in the system and the organizational and operational cultures that many grid operators have.

"It can be a bit of a hardship—a lot of these organizations, specifically in the SCADA realm, are change averse," Sigler says. "They are not the most agile when it comes to patching; they generally follow the if it's not broke, don't fix it approach. They're dealing with extremely critical systems, and if you install a patch on a SCADA system and it crashes components, you can be talking about causing more damage than the patch was supposed to fix."

Sigler also adds that Trustwave's findings are similar to other vulnerabilities that have been reported in the past decade after the Stuxnet cyberattack became public, explaining that vendors' responses are encouraging because it reflects a mind-set change that simply preventing hackers from gaining access through air-gapped networks is not enough to protect systems.

"We've seen a lot of these vulnerabilities in the past," he says. "I think that all these vendors are quickly coming around to the realization that they need to be better—having their own software that's internally secure and not relying on external controls to prevent exploitation."

directed towards critical infrastructure and industrial entities as geopolitical tensions rise. It identified similar tactics during summer 2019 among the United States, Saudi Arabia, and Iran.

Dragos also analyzed that the threats to ICS are becoming increasingly numerous and sophisticated as threat actors invest resources to obtain the ability to disrupt critical infrastructure. For instance, the activity group XENOTIME (which was behind the TRISIS malware that targeted Schneider Electric's Triconex safety instrument system) engaged in a pattern of attempting to gather information and network resources associated with U.S. and Asia-Pacific electric utilities.

"XENOTIME expanded its probing activity to include electric utilities, using the same techniques previously deployed against oil and gas entities," according to the report. "Additionally, as identified in previous Dragos reporting, XENOTIME has targeted, and in some cases successfully compromised, original equipment manufacturers, potentially impacting the entire industrial supply chain."

The report also identified an increase in malware infections, such as ransomware, at industrial companies in 2019.

"The malware and ransomware incidents largely target enterprise networks," according to the report. "However, like Dragos has observed multiple times, incidental infections within the OT due to poorly segmented or misconfigured networks, or infections disrupting IT software or services required for operations—like data, fleet, or production management software—can have operationally disruptive effects."

Along with new and developing tactics, threat actors are also using common and popular tactics to gain access to their target's ICS, such as password spraying—when adversaries target numerous accounts using common passwords to attempt large-scale authentication to gain access.

We thought federal assessments of the impact had limitations.

"Although password spraying is a relatively common technique attackers use to gain access to enterprise resources, organizations are often vulnerable to these types of attacks because of poor account management and authentication policies for external resources," according to the Dragos report.

The report also identified instances of threat actors using phishing campaigns to target ICS entities. For instance, actors used LinkedIn direct messaging to send "project proposal" lures. "LinkedIn can be a useful phishing route for an adversary as it can bypass email security filters and attackers can leverage users' network connections to appear as a legitimate contact," the report explained. (See "The Cost of a Connection," *Security Management*, February 2019)

Impact

In response to some of GAO's grim assessments, the U.S. government and North American regulators have taken action to increase grid security.

In early 2020, U.S. President Donald Trump signed an executive order to enhance security of the U.S. bulk-power system. A primary focus of the order was limiting foreign supply of the system's electric equipment, a measure that would address in some part the supply chain threat identified by the GAO.

Under the order, operators are prohibited from purchasing or installing bulk-power system electric equipment where the transaction involves any property that a foreign country or national has interest in and poses an undue risk of sabotage or catastrophic effects on the security or resiliency of U.S. critical infrastructure or the economy of the United States.

The order also grants the authority to the U.S. secretary of energy to create criteria for recognizing equipment and vendors as prequalified for purchase and installation into the U.S. electric grid.

In the GAO report, auditors recommended that the DOE develop a plan to implement a federal cybersecurity strategy for the electric grid and include a full assessment of cybersecurity risks to the grid.

DOE agreed with this recommendation and said in a statement included in the GAO report that it is working with the National Security Council to develop a National Cyber Strategy Implementation Plan.

The North American Electric Reliability Corporation (NERC) also released a suite of cyber standards for some—but not all—grid operators to comply with over the course of the past decade (CIP-002 through CIP-011). NERC is the international regulatory authority that develops and enforces reliability standards, assesses seasonal and long-term reliability, and monitors the bulk power system in the United States, Canada, and the northern part of Baja California, Mexico. It is overseen by the FERC and Canadian government authorities.

Howard Gugel, vice president of engineering and standards for NERC, says that the regulator began developing a suite of cyber standards using a risk-based approach and assessment methodology to help operators determine what their risk was and apply controls to reduce it. This resulted in several standards, along with a recent revision of a standard: CIP-008-6, *Cybersecurity—Incident Reporting and Response Planning*.

The previous standard only required operators to report all compromises to their systems. It did not require operators to report attempts to compromise, which meant there was a lack of understanding of the threat landscape, Gugel says.

"These standards have been in place for years, so it was time to say, 'Let's start looking at some attempts—maybe we can reduce some shots on goal,'" he adds.

Under the updated standard, which goes into effect on 1 January 2021, subject grid operators will be required to report all cybersecurity incidents. NERC defines an incident as "any malicious act or suspicious event that compromises or was an attempt to compromise the electronic security perimeter or physical security perimeter of a critical cyber asset, or disrupts or was an attempt to disrupt the operation of a critical cyber asset."

The SANS Institute's Conway says that having terms like "incident" defined and a set scope of regulations addressing cybersecurity is a benefit to the electric operator community.

"Previously, asset owners and operators could define what a reportable incident was," Conway explains. "If someone broke into a control center and disrupted the [system], that's a cybersecurity incident. But if it didn't cause any effect on power generation, dynamic response, any type of situational awareness, or control center functions, it wouldn't have been reportable."

Operators must also provide evidence collected on the incident, including documentation that demonstrates maintenance of each incident response plan in accordance with the standard. Owners must then notify the Electricity Information Sharing and Analysis Center (E-ISAC) of the incident.

U.S.-based operators are further mandated to report this information to the U.S. National Cybersecurity and Communications Integration Center (NCCIC). There is no similar requirement for Canadian-based operators.

Additionally, all subject operators are required to provide continuous updates about the incident within seven days of learning something new. They must also detail what the functional impact of the incident was, for instance what the threat actor was likely targeting.

Penalties for noncompliance with the updated standard will be determined on a case-by-case basis, Gugel says.

"We do an assessment of the situation with our compliance and enforcement folks, take into account the scenarios that occurred, mitigating effects put into place—that's all evaluated," he explains. "If determined there's a penalty, then that's developed and put forward. There is not a cookie cutter automatic fine."

Gugel says he is not aware of any other regulatory authorities that have adopted similar standards for electric grid operators, but many countries are using NERC's standards as a model for what they would like to implement.

"Our standards are the minimum requirement; we expect entities to do at least that," Gugel says. "Our entities put other controls in place. These are just the ones that we say have to be done."

Based on its analysis, the GAO recommended that FERC consider adopting changes to its approved cybersecurity standards to more fully address the NIST Cybersecurity Framework.

The GAO also recommended that FERC evaluate the potential risk of a coordinated cyberattack on geographically distributed targets and determine if it needed to change the threshold for mandatory compliance with its full set of cybersecurity standards.

FERC Chairman Neil Chatterjee responded to the recommendations in a statement and said he considered them "constructive" and has directed staff to take appropriate steps to implement them.

Rusco says that FERC, as of *Security Management*'s press time, was conducting studies on applying the NIST Cybersecurity Framework to its standards and on effects of coordinated cyberattacks. But despite these actions, regulators, government agencies, and operators will need to remain focused on cybersecurity across the grid.

"You are only as strong as the weakest link," Rusco says. "Given that everything is becoming more and more interconnected, you're going to have to massively train everyone who uses equipment that's vulnerable to watch out for hacks. Or you're going to have to have systems that are able to expand into a broader and broader landscape where everyone has more devices that are Internet connected and connected to other things. We're heading into unchartered waters." ■

MEGAN GATES IS SENIOR EDITOR AT *SECURITY MANAGEMENT.* CONNECT WITH HER AT *MEGAN.GATES@ASISONLINE.ORG.* FOLLOW HER ON TWITTER: *@MGNGATES.*

The Intersection of Sustainability and Security

An unusual combination of sustainability, safety, and security aids Radisson in becoming a more trusted member of both global and local communities.

"Think People, Think Community, and Think Planet." These three pillars drive Radisson Hotels' joint safety, security, and sustainability missions, helmed by Inge Huijbrechts, global senior vice president for safety and security and responsible business at Radisson Hotel Groups. Combining safety, security, and sustainability under a single senior vice president may be unusual. However, in the face of growing global uncertainty and changes, the insight this lens can provide a global enterprise is invaluable—especially when backed by a high-functioning team of hospitality-minded specialists.

The program, Huijbrechts says, only really works when paired with engagement from employees, owners, and key partners.

After more than two years in the role of managing the joint mission, Huijbrechts finds the combination effective, and with the coronavirus pandemic, she says she knows ensuring that safety and organizational recovery needs to be sustainable for long-term success.

The following conversation has been edited for clarity and length.

What does the combination of security and sustainability look like? What does "responsible business practices" mean to Radisson, especially with regards to sustainability?

IH. For us, responsible business means that we try to be a responsible company in everything we do. We focus on three pillars, called Think People, Think Community, and Think Planet. Think People means that we always care for the people in our hotels and our supply chain. So, in our outwards communications, safety and security was always part of the Think People focus area. Making sure that we welcome guests in a safe and secure environment in our hotels is essential, so it was always part of our responsible business report to talk about safety and security as part of Think People. Think People is also everything we do on business ethics, on responsible supply chain management, and on our people development, so it touches on the work of our HR teams in terms of developing people.

Think Community is caring and contributing in a meaningful way to communities where we operate. We also contribute to communities in the areas of food, shelter, and a better future, so it entails everything in terms of providing employment and employability opportunities for young people and people who are in difficult situations. We donated €1.6 million ($1.8 million USD) last year to various nonprofits, we volunteered 43,000 volunteer hours—these kinds of elements all fall under our meaningful contribution to our community.

Finally, Think Planet makes sure that our footprint on the environment is as light as it can be in terms of energy, water, waste, and carbon, and making sure that we incorporate sustainability into our value proposition to the guests. For example, we've reduced our carbon emissions per square meter by 16 percent since 2017, and before that we had very successful energy consumption reduction. Since 2011, we've reduced our energy consumption and our water consumption by 30 percent, so those are significant actions to reduce even though we grew as a company. We have, for example, carbon-neutral Radisson meetings, which means that any meeting or event that takes place at a Radisson hotel is automatically carbon neutral.

How does one function inform or influence the other, and how does the intersection of these two departments influence your decision making?

IH. When you talk about responsible business, sustainability, and safety and security, they are very much expert environments. You need a team of experts who are in service of our hotels.

The other aspect that is essential is that they both can only be successful in a large hotel company if you get the engagement of all your hotels and all hotel teams. You can never force these things; you have to get the engagement of the employee base of your hotels, of your owners, of your key partners.

And the last part where they are linked is also on a geopolitical level. If we as a company know how to operate more responsibly in a location, we can gain the trust and the license to operate, which in turn then makes us more safe and secure as a business. On the other hand, for example, if you develop hotels in locations that see the impacts of climate change, you will see water security issues, you will see safety issues originating from your climate change. Those two, in terms of risks to the business, in terms of geopolitical or climate change risk, those are very much intertwined.

What do you look for when you're putting together a team for these functions?

IH. I think I inherited a great team who are all people who have hospitality in their veins, which means this attitude of "Yes, I can." You need to be serving the guests, serving the hotels, serving your colleagues, and you need to have that service mind-set in everything you do. If you want to get that engagement of your teams, which is so essential to making hotels safe and secure and making sure that everybody practices responsible business in their day-to-day job, you can only do that when you have a service mind-set yourself.

And then, of course, they need to have a broad view, and that's quite unique. We combine safety and security under the same department, and then you add sustainability, so, we have to have people who can understand this broad spectrum. We don't have a big team, so people need to have that generalist understanding on top of their special expertise.

What risks are important or a priority regarding sustainability? Why is this important for the security industry?

IH. The impacts of climate change. That's it.

We have resources in general, but in our 24/7 business, you can't operate without energy, you can't operate without water, you can't operate without a stable food supply chain, and you can't operate without your team. So, the availability and the stability of all those aspects are essential in terms of risk management. That's where we have a responsibility to have our footprint as light as possible in terms of resource use, as local and as stable as possible in terms of food supply, and as long-lasting, sustainable, and responsible as possible in terms of caring for the workforce.

Because if we care for our workforce in a correct way, every person you employ in a developing country ensures more financial stability for a wider group. It's not about that one person, it's about their family, it's about their network that you helped sustain through a responsible job. They are not just sustainability risks, they are security risks as well.

How did you convince the C-suite that this combination was an asset to the company?

IH. I think that was kind of a gamble and, to be honest, it took a while to convince people who expect security to be only focused on the expertise that a lot of people have coming out of the military or coming out of intelligence services, police, or diplomatic security. But you see in the security world that there's more of a shift away from that very strong expertise to a more global view on security.

It took time internally to convince certain people that somebody without the expertise of law enforcement, military, or the intelligence community could actually lead security and safety. But of course, I could not lead this on my own. You need a team of experts who help you with this and who will work with you as a team to make it work. To set a meaningful strategy and understand how these departments serve the business, you don't need to be a specialist—you just need to see how they work together and how you can help by bringing them together.

You can, I would say, bring a perspective that is broader but also at the same time shows that you can handle, as a leader, a crisis and that you cooperate across the business. The trust from the business itself was rapidly there, so our operational leaders trusted this move quite quickly because they had seen me in action as a leader for responsible business in connection with operations. It was more the C-suite who was thinking in silos, and some had difficulty seeing that this would work. I think the proof came through certain crises and taking the company through those crises.

What fundamentals should a business leader focus on if they want to incorporate or merge sustainability into security?

IH. The first thing is to pitch it from a strategic level, because you need to pitch it to the leaders of your company. That's a very strategic conversation to have, but in terms of having conversations with operational leaders, with finance, with insurance risk functions, this totally makes sense.

I think it also makes sense in a service business like ours because it's so people-centric, and if you have that mind-set, I think you can start combining. Keep in mind that you will need experts in sustainability, in community engagement, ethics—you need to bring those fields of expertise under the same leadership.

> *"You break down the silos and you look at things holistically, and many of the global issues need a holistic approach."*

I think a first step to move in that direction is already making sure that as part of your sustainability and responsible business reports, there's also a mention of safety and security.

When you're dealing with global-scale issues—like impacts of climate change, the impacts the pandemic will have on food security and the rise of crime, and preventing modern slavery and the impacts that can have on hotels—all these things that have global impact, you need to approach them in a holistic way.

What are some of the benefits to hotel security or business continuity that sustainable practices and/or responsible business practices can provide?

IH. I think it's a matter of efficiency and credibility of a responsible company. You break down the silos and you look at things holistically, and many of the global issues need a holistic approach.

What helped is whenever I look at a risk now—with a growing expertise in safety and security—you actually look at things from a different angle. For example, in Freetown, Sierra Leone, three months after we opened a new hotel there, the Ebola crisis hit.

When a new hotel opens, it takes time for business to pick up—it takes usually a year. The gentleman running that hotel kept all the staff they had hired, trained them, and he and others agreed to reduce their salaries to do so in a responsible and ethical way. So, he kept the team together and safe, and he kept their families safe, because he trained everybody on how to prevent Ebola. That contributed to a more secure situation, as well, and the hotel recovered business. They had built that reputation of trust in their community so that it contributed to the safety and security of the place.

One of our hotels in Bangladesh contributed on a regular basis to the local community. They involved the local community with their local projects, whether it's around food donations, clothes donations, trainings, employability—in doing so, they actually built that trust in the local community. So that means that the hotel becomes a safer place to be, even if you're in an emerging market, because you do the right thing in terms of responsible business and safety and security.

They influence each other on a micro level, but they also influence each other on a macro level. When we look at the coronavirus pandemic, we know there's going to be instability in a lot of places. By being a responsible citizen in these places, we are going to build trust, and the trust is going to be needed for our business to operate successfully again in those local communities. ▨

SARA MOSQUEDA IS ASSISTANT EDITOR AT *SECURITY MANAGEMENT.* CONNECT WITH HER AT *SARA.MOSQUEDA@ASISONLINE.ORG.*

What's better than providing meals to people in need?

Providing 1 Million Meals!

FEEDING AMERICA™

Mission 500 has launched the Million Meal Challenge in partnership with Feeding America to assist families in need across the U.S. who are struggling as a result of the coronavirus pandemic. We're calling on all our peers across the professional security industry to help raise $100,000 to fulfill this goal. There are many ways to contribute whatever you can during these unprecedented times. Every single donation helps. **For more info please visit Mission500.org**

Supporting Families Across America

MISSION 500

For product info #17 securitymgmt.hotims.com

Security in

Robust security technology, guarding programs, and threat assessment programs can fall flat when implemented without one essential element—contextual intelligence.

You are the recently appointed chief security officer of a major multinational corporation. You have more than 20 years of upper-level law enforcement experience in your home country, and your first major project is a review of the company's Tokyo facility. A team of experts and vendors has been put together to review the threats specific to the locale and the vulnerabilities of the facility.

Months of analysis and review have gone into the project. Additional time has been spent installing perimeter upgrades, baggage and parcel screening technology, and magnetometers. Dedicated and guarded employee parking areas have been constructed and operationalized. More than $250,000 has been invested in hardware alone.

Finally, the project is complete. You have contracted a local security professional to conduct a red team active review of the installation to measure its effectiveness. No more than 15 minutes after the start of the test, the expert calls you from the executive conference room, having bypassed the entire physical security system you worked so hard to put in place.

When asked how this was achieved, the penetration tester replies: "I copied

Context

PHOTOS BY ISTOCK

the company's logo from the Web, used a color printer and laminating paper to make a simulation of a badge, and told the front desk that I had flown in from U.S. corporate for an emergency audit meeting. I said that the CEO demanded that I start immediately, and I do not know why my ID card does not work. They let me right in and led me to the conference room."

In implementing the sophisticated physical security measures, the CSO neglected to consider one thing: the culture of the workers, who were reticent to confront an individual who claimed to be in a position of authority.

Culture and Contextual Intelligence

Culture is one of many elements that today's security professionals must consider to successfully navigate redefined boundaries related to geography and diversity, and even in relation to education, experience, and expertise.

Incorporating the impact of culture in decision making exemplifies the application of contextual intelligence—a concept used for decades in the management and sports sectors—to contemporary security practices.

Context is the background against which an event takes place; it makes information meaningful. Intelligence about context enhances situational awareness and enables more relevant, efficient, and practical decisions.

A great deal of attention has been given to affective or emotional intelligence, which focuses on the realm of moods and feelings. It was originally formulated by psychologists Peter Salovey and John Mayer, and popularized by psychologist and science writer Daniel Goleman.

Emotional intelligence focuses on self-awareness, self-control, and empathy. Improving one's understanding of emotional intelligence is often promoted as a necessary skill set for improving people management and job performance. (For more information, see "Harnessing the Power of Emotions," *Security Management*, September 2015.)

Contextual intelligence, coined in 1984 by Yale University psychologist Robert Sternberg, is a cognitive process that involves thought, understanding, and perception. Contextual intelligence prioritizes the environment, relying upon three primary processes to optimize decision making: adapting to the environment to meet our objectives; shaping the environment to meet our objectives; or selecting to abandon a project altogether.

Different industries have employed various methodologies to determine whether it's best to adapt, shape, or abandon endeavors.

In the security sector, we recommend a simple framework, encapsulated by the mnemonic COPE—culture, organizational values, politics, and environment—to apply contextual intelligence to enhance decision making at the executive and managerial levels and on the front lines.

Contextual Intelligence in Action

Contextual intelligence is pragmatic and allows for nuancing the all-hazards approach to more effectively prepare and respond to security risks. Incorporating contextual intelligence into a proven threat assessment model enhances its efficacy.

Context is the background against which an event takes place; it makes information meaningful.

Culture, the first element of the COPE framework, can be defined as the customary beliefs, social norms, and racial, religious, or social group characteristics shared by people in a place or during a time.

In the Tokyo security example above, an understanding of the deferential culture of the employees responsible for the reception areas might have mitigated the security breach during the penetration test. In response, the organization could have adapted the environment to eliminate the need for staffed entrances or shaped the environment through targeted training of frontline security.

In his primer for army personnel on the front lines in Iraq and Afghanistan, U.S. Lieutenant Colonel William D. Wunderle offered the example of U.S. troops forcing the heads of Iraqis to the ground during arrests—an act which violates Islamic religious norms of not allowing the head to touch the ground except in prayer. Behaviors that offend cultural norms can undermine core security missions; in the case of the global war on terrorism, offending detainees and the populace who witnessed the arrests threatened to undermine the mission of bringing stability to the Middle East, Wunderle said.

However, research on cultural competence across disciplines has found that knowledge of norms and customs is but one element to being successful. The capacity to assess one's own cultural biases, to value diversity and manage differences, and to accommodate another's worldview are also key. The deeper understanding of another's perspective—derived from cultural competence—enhances the ability to predict behavior.

Priorities and Values

The second element of the COPE mnemonic, organizational values, seeks to ensure that any security plan, decision, or response aligns with institutional priorities. Consistent with the enterprise security risk management (ESRM) approach, the consideration of organizational values as a facet of contextual intelligence supports transcending security silos between people, assets, and processes, and between security and business outcomes.

Efforts to replace the so-called school-to-prison pipeline phenomenon in the United States with alternative classroom management approaches exemplify consideration of organizational values in action.

Highly publicized active assailant incidents in public and private schools in the past decade have given rise to two dynamics that have contributed to higher arrests of schoolchildren: an increase in the number of school resource officers (SROs), and a decrease in tolerance levels for disruptive classroom behavior, which is often regarded as a high indicator of risk for violence.

An increasing number of institutions are seeking security solutions that are more congruent with their educational values. Alternatives—such as restorative justice, which emphasizes accountability, peer learning, and meditation in response to unacceptable behavior—are being explored.

SROs can be instrumental in these efforts, adapting their expertise in de-escalation, risk communication, and behavioral threat assessment to support safety without criminalization. Considering factors such as age, developmental level, and social status within the school environment can contextualize benign behaviors that might otherwise be perceived as threatening or insubordinate.

Political Context and Environment

Politics—the third element in the contextual intelligence mnemonic—is defined here as the larger context in which a situation is occurring and the specific influences that may need to be evaluated.

Consider events in China in 2008. After an earthquake destroyed 67 percent of the habitats of China's beloved panda bears, a type of panda mania set in worldwide. Pandas are typically popular—researchers suggest pandas activate regions in human brains like those triggered by human infants (recall their snub noses, wide cheeks, and toddling gaits)—but the events of 2007 sparked a surge in merchandising.

Against this context, it was perhaps not completely unsurprising when a 20-year-old student visited Qixing Park in Guilin, China, and scaled a 6.5-foot wall to enter the panda enclosure. He was repeatedly bitten by Yang Yang, one of the zoo's pandas, before being rescued by zookeepers. The student subsequently claimed that he "just wanted to cuddle" the panda, according to the official Xinhua News Agency.

The larger political context at the time—in this case, a heightened interest in pandas—might have suggested that relying on a 6.5-foot barrier and the common sense of visitors might not be adequate to achieve a primary security objective of maintaining separation between humans and the very popular pandas. The environment and its security might have benefited from being shaped to match the larger political context.

In contrast, environmental context refers to local events and influences.

The impact of environment on security during the current COVID-19 pandemic is exemplified by an early effort by a southern California public–private partnership. In March 2020, the collaborative unveiled plans to slow the virus's spread by treating potentially coronavirus-positive homeless patients at vacant hotels. One of the chosen facilities was proximate to a community of 18,000, many of whom were in the high-risk 65 and older age group.

The result was a series of protests, online petitions, and dissemination of misinformation. A plan that worked perfectly across multiple environments was not adapted to the local conditions of an older community and resulted in civil disobedience and multiple security risks.

In contrast, a community health center—mindful that its surrounding neighborhood generally responded to change with anxiety and unrest—opted to test potential COVID-19 patients discreetly; rather than erecting a parking lot tent, patients were tested in their cars. The healthcare response was adapted based upon the environmental context.

Can Contextual Intelligence Be Taught?

Traditionally, it has been believed that contextual intelligence could not be taught directly: You either had it, or you didn't. But research in various areas—most notably business and sports psychology—has helped debunk this myth.

As industry globalized, business schools recognized the necessity of ensuring that future industry leaders understood contextual intelligence if businesses were to succeed in emerging markets. Tarun Khanna, economic strategist and Harvard Business School professor, used the example of a cement factory.

He pointed out that although the process for making cement is consistent across factories, the context in which a factory is embedded can influence everything from whether corrupt suppliers adulterate mixtures, to whether workers are unionized, to the way in which the final product is sold locally. The company seeking to relocate a plant to a location that might appear to offer greater return-on-investment potential must understand the impact of the contexts in which the business will operate.

Over time, the incorporation of contextual intelligence on business curricula and, subsequently, practices have allowed for interesting innovations. Popularized by sociologist Roland Robertson, "glocalization" can be viewed as the adaptation and shaping of contextual intelligence in action. It has resulted, for example, in one's ability to purchase both a Big Mac and Seaweed Shake Shake Fries when at a McDonald's in Hong Kong.

Likewise, sports psychology teaches its practitioners to intentionally consider the context in which they are working with athletes—the culture of the team and the sport, the values of the league, politics surrounding sponsorship, and the influence of local fans—to support maximum individual performance in their clients.

Incorporating contextual intelligence into a proven threat assessment model enhances its efficacy.

Teaching COPE in Security

Contextual intelligence can also be taught and learned at all levels of the security team by integrating COPE factor analysis into relevant decision-making processes.

On the front lines, this occurs through COPE inclusion in various drills, thought experiments, and operational templates. It involves movement beyond standard—and frequently superficial—training in cultural competence to training that has greater relevance, depth, and impact.

The use of case studies, for example, allows security professionals to develop knowledge of cultural nuance and test their ability to predict behavior based upon this knowledge. Then they can compare their predictions against real world results.

For example, are frontline security professionals for a hypothetical Malaysian e-commerce company able to detect and prioritize potentially significant nuances related through case studies: What is different today from yesterday? Are children playing in the neighborhood as normal? Are they suddenly gone? Are there new faces in the area? Have local radio stations increased negative mentioning of internationals? Has the village matriarch invited you to take tea, as usual? Or, are there more males and fewer females present than normal?

What does the subtle presence of the cultural normal or its absence potentially mean? Conversely, what does the presence or absence of that which is culturally incongruent signify? What could these subtle changes signal?

This approach can also uncover implicit biases that most of us hold—and about which we are typically unaware. In at least some areas, unrecognized biases can impede successful decision making.

A bias, for example, that men are more lethal than women can create a vulnerability if an organization dismisses early warning signs from a high-risk female.

Managing with COPE

On the managerial level, the inclusion of COPE factors assists in professionalizing the workforce, connecting members of the security team more closely with organizational missions, and providing a forum to review the often shifting macro- and micro-influences that affect the provision of services in various industries.

COPE may cause managers of security at a large metropolitan hospital, for example, to shift a drill's focus from active assailants to workplace domestic violence or a pandemic based upon a sensitivity to the hospital system's culture and organizational values of supporting the physical and psychological safety of its workforce, coupled with an ongoing analysis of threats in large hospital systems regionally, as well as the emergency department specifically.

At the executive level, COPE provides a framework for both considering and informing critical institutional decision making by casting security intelligence in the broader themes that are vitally important to an organization's ability to survive, particularly during times of change or complexity. Using the COPE framework, for example, may inform recommendations to abandon reallocating resources from current security efforts—which can be demonstrated to align with culture, organizational values, and current political and environmental events—over a security proposal that has limited or no utility to the institution's larger goals.

Can Contextual Intelligence Be Assessed?

Assessing the contextual intelligence of security job applicants can be achieved through case studies that evaluate contextual sensitivity. Industry-specific hypotheticals that require the candidate to articulate the factors they would consider when engaging in decision making can assess contextual intelligence.

Psychologist Robert Sternberg offered the following example of operationalized contextual intelligence in a workplace setting.

An employee loved his work, coworkers, and where he lived, but hated his boss. The employee was contacted by a recruiter who had heard of his dissatisfaction and offered him a position with considerably more pay and responsibility at a company in a nearby city. The employee declined the position and instead gave the recruiter his boss's name. His boss took the job.

Sternberg's example demonstrates each of the factors suggested by COPE—cultural consideration, an evaluation of the role of organizational values, politics, and the environment—to arrive at a pragmatic and creative solution.

To see how contextual intelligence can be leveraged in a security setting, consider the following anecdote.

Doctors and mental health workers at a maximum-security penitentiary are threatening to strike, claiming safety concerns stemming from a lack of rapid response by correctional officers to panic calls. They cite two staff who were badly injured over the prior three-month period. Correctional officers, in response, report that the majority of calls by workers are false—either made by accident or never received. A strike would threaten the facility's ability to provide needed care to inmates and obtain a coveted accreditation status, and it could generate negative publicity. What factors would you consider when developing a security solution to this situation, and what potential resolutions do you envision?

Applying the COPE framework supports an evaluation of the security candidate's response. Does the candidate consider the potential cultural differences between medical and correctional staff and offer thoughts on ways to bridge any possible divide? Does the proposed response include an investigation of the institution's values and priorities, perhaps identified through how it managed the incidents with the injured workers? What are the political ramifications of obtaining—or losing—the specialty accreditation? And, have there been recent local or sector-specific news events that render the institution particularly vulnerable to negative publicity at this time?

A contextually intelligent applicant will likely respond to such a scenario in a way that moves beyond a limited focus on modifying equipment (a simple abandonment of the current hardware) to a more sophisticated plan that includes adapting to and/or shaping the current environment. For instance, the development of scaled responses based upon inmate risk levels, with the establishment of special joint healthcare–correctional officer deployment teams for the highest risk populations.

The Contextually Intelligent Security Team

Contextual intelligence and the COPE framework support the professional development of individual security personnel—whether in the C-suite, at the managerial level, or on the front lines—through the enhancement of decision-making skills.

Training members at all levels of the security workforce also supports the establishment of a consistent problem-solving approach that can unify diverse members of a security team, improving the ability to coordinate and collaborate across roles.

In this way, a shared commitment to considering culture, organizational values, politics, and environment to inform whether to adapt, shape, or abandon situations promotes the contextually intelligent security team's capacity to successfully meet today's complex security challenges. ▨

DR. DIANA M. CONCANNON IS A FORENSIC PSYCHOLOGIST, ASSOCIATE PROVOST AT ALLIANT INTERNATIONAL UNIVERSITY, AND DEAN OF THE CALIFORNIA SCHOOL OF FORENSIC STUDIES. SHE IS SPECIAL ADVISER OF ASIS INTERNATIONAL'S PROFESSIONAL DEVELOPMENT AND SCHOOL SAFETY AND SECURITY COUNCILS. **MICHAEL CENTER** IS A REGIONAL SECURITY ADVISOR FOR THE UNITED NATIONS DEPARTMENT OF SAFETY AND SECURITY BASED IN BRUSSELS, BELGIUM. HE IS CHAIR OF THE ASIS PROFESSIONAL DEVELOPMENT COUNCIL AND CO-VICE CHAIR FOR SUBJECT MATTER EXPERTISE OF THE GLOBAL TERRORISM, POLITICAL INSTABILITY, AND INTERNATIONAL CRIME COUNCIL.

THE VIEWS EXPRESSED IN THIS ARTICLE ARE THE AUTHORS' OWN AND ARE NOT REFLECTIVE OF THEIR ORGANIZATIONS.

THE EXPERIENCE YOU RELY ON FROM GSX...

+ CONNECTIONS

Interactive group activities and one-on-one attendee matchmaking to encourage relationship building across the security community.

+ COMMERCE

A unique and interactive marketplace to meet exhibitors and demo the latest products in an easy-to-use, safe, and secure platform.

+ CONTENT

80+ education sessions covering the latest in today's complex and rapidly evolving enterprise security risk management landscape. Plus, earn up to 25 CPE credits.*

+ COMMUNITY

Further support the beterment of the industry at the ASIS Hub which directly supports the funding of scholarships for security professionals around the globe.

*25 CPE credits available per all-access pass.

…NOW GLOBALLY AMPLIFIED AT GSX+

Through a new virtual platform, GSX+ opens doors to a world of opportunities and answers for professional development and collaboration, expanding your perspectives on the future of physical and cybersecurity, facilities management, crisis management, and business continuity planning.

GSX+

GLOBAL SECURITY EXCHANGE PLUS

21–25 SEPTEMBER 2020

REGISTER TODAY AT GSX.ORG/EB

Use code EARLYPLUS for $75 off an all-access pass.

INTRODUCING GSX+

FOLLOWING MONTHS of careful evaluation of the risks associated with convening 20,000+ professionals from around the globe during the COVID-19 pandemic, ASIS leadership concluded that cancelling the live Global Security Exchange (GSX) 2020 event was the correct course of action—in the best interests of ASIS's members, attendees, speakers, exhibitors, and the public.

Enter Global Security Exchange Plus (GSX+). Taking place 21–25 September, this new, virtual experience includes more than 80 industry-leading security education sessions, a robust marketplace, and unique peer-to-peer networking opportunities.

"While circumstances dictate that we must forgo an in-person meeting this year, we are excited for GSX+ to deliver to a wider global audience the exceptional security networking, marketplace, education, and training that truly set GSX apart," says Godfried Hendriks, CPP, president of the ASIS Global Board of Directors. "There is a growing demand for a comprehensive experience that helps the entire security profession learn and grow together." GSX+ will deliver every element of a live event in an online environment: community, content, commerce, and connection. Without any necessary travel, GSX+ offers the global community of security professionals a forum to gather for important real-time conversations about trends, best practices, and the future of the security industry.

Topics of GSX+ education sessions will range from workplace violence and behavior detection to return to work, pandemic lessons learned, and well-being of security personnel.

"The new GSX+ will deliver more continuing professional education credits (CPEs) than GSX, more accessibility with a lower cost to participate, and GSX+ edu-

GSX+ FREQUENTLY ASKED QUESTIONS

How will GSX+ support networking events?
The GSX+ platform will allow participants to network with peers through one-on-one meetings, small group discussions, and larger networking events.

Look for tutorials on using the platform to be shared closer to the event.

How can I experience new security technologies at GSX+?
Through the GSX+ Marketplace, attendees can engage companies directly and request private meetings or product demos, watch on-demand or live scheduled product demos and tech talks, and more.

cational content will live online for several weeks after the experience concludes," adds ASIS CEO Peter J. O'Neil, FASAE. "It's never been more important for organizations to focus on risk management and business continuity. GSX+ offers a new way for professionals to come together, discover new technologies and approaches, and dive into important discussions around global best practices."

For more information about the GSX+ experience, visit *GSX.org*.

SECURITY INDUSTRY BOOK OF THE YEAR

ASIS International's 2020 Security Industry Book of the Year is *Strategic Security: Forward Thinking for Successful Executives* by Jean Perois, CPP.

In *Strategic Security,* Perois argues that security professionals too often approach their roles through a reactive lens rather than a proactive one—serving more as "firefighters" than as strategists. The book looks to help security managers think strategically about their job, the culture of their workplace, and the nature of security planning and implementation.

"This book is a great read for any current or aspiring manager," ASIS member Yan Byalik, CPP, shared during a review in the February 2020 issue of *Security Management*. "It provides an excellent discussion on building or being prepared to lead a successful security organization."

Now in its seventh year, the Security Industry Book of the Year is chosen by a committee of ASIS members who are established authors, editors, and reviewers. Eligible books were authored by ASIS members and published in 2019.

"*Strategic Security* by Jean Perois provides a much-needed high-level strategic guide that is perfectly balanced with sufficient details to guide practitioners in developing a security master plan that will achieve the desired results," explains Steve Van Till, CEO of Brivo and chair of the Book of the Year Committee. "It is also both politically and psychologically astute in advising how to pursue one's goals with the mix of personalities, motivations, and viewpoints that are a part of every large organization. It could well be the one book every practitioner should read at the beginning of his or her career."

Twenty-four books were considered for this year's award. The committee chose two finalists from the contenders. The other finalist was *Security Management for Healthcare: Proactive Event Prevention and Effective Resolution* by Bernard J. Scaglione, CPP.

Security Management for Healthcare highlights the need for healthcare facilities to have policies and procedures that require reporting of threatening or unusual behaviors. Having preventive policies and procedures in place is the first step in mitigating violence and providing a safe and secure hospital.

These books—and other books published by ASIS members last year—are

GSX+

How many CPEs are available for attending GSX+?

- All-Access Pass: 25 CPEs (includes sessions, Marketplace, and on-demand recordings)
- One-Day Pass: 5 CPEs per day (sessions and Marketplace)
- Marketplace-Only Pass: 5 CPEs

What if I miss a live education session? Will sessions be recorded?

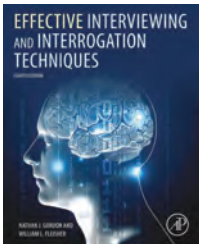
GSX+ sessions will be recorded and available to All-Access registrants through 31 December 2020.

Learn more at *GSX.org/FAQs.*

available online in the ASIS Store. Visit *store.asisonline.org* to find these publications and more.

MEMBER BOOK REVIEW

Effective Interviewing and Interrogation Techniques, Fourth Edition. **By William L. Fleisher and Nathan J. Gordon.** Academic Press; *Elsevier.com;* 406 pages; $125.



While law enforcement, loss prevention, and security experts can learn something from this book, the general public can, too. Its clear, easy-to-read structure will help HR professionals, attorneys, and security practitioners who are tasked with interviewing people and finding truth in the written and spoken word. The authors of this fourth edition of *Effective Interviewing and Interrogation Techniques* provide a brief overview of the history of interviewing and interrogation and then jump right into the purpose of the book: to make the reader more proficient in searching for the truth.

The authors lay out in detail the steps needed to obtain accurate information from individuals. Included in this process is an understanding of the psychophysiological basis for the assessment as well as techniques that an interviewer can use.

#MYASIS IMAGE OF THE MONTH

ASIS PERÚ

Muchas gracias a todos los miembros y líderes de ASIS International, expositores y comunidad de seguridad en general por su apoyo y participación.

BOOKS BY ASIS MEMBERS PUBLISHED IN 2019

An Introduction to Operational Security Risk Management
Tony Zalewski

Unwavering: A Border Agent's Journey from Hunter to Hunted
Dr. Jason Piccolo, CPP

P.A.C.E.: Active Shooter Workplace Violence Preparedness (Prepare, Act, Care, Evacuate)
James Cameron, CPP

Security Management for Healthcare: Proactive Event Prevention and Effective Resolution
Bernard J. Scaglione, CPP

The Chief Security Officer's Handbook
Michael Allen

Effective Interviewing and Interrogation Techniques, Fourth Edition*
William L. Fleisher and Nathan J. Gordon

Strategic Security: Forward Thinking for Successful Executives
Jean Perois, CPP

School Security: What Works, What Doesn't and Why
Charles Schnabolk

Engineering Practices and Security Technology
Charles Schnabolk

The Protected
Michael Trott

Casino and Gaming Resort Investigations
Derk Boss, CPP, and Al Zajic, CPP

Private Security and the Investigative Process, Fourth Edition
Charles P. Nemeth

*Reviewed in this issue

Strategic Security Management, Second Edition
Karim Vellani, CPP

Violence Assessment and Intervention: The Practitioner's Handbook, Third Edition
James S. Cawood, CPP, PCI, PSP, and Michael H. Corcoran

Lead, Follow or Get Out of the Way: Inspirational Stories and Quotes About Leadership, Courage and the Remarkable Human Spirit
Jonathan D. Rose, CPP, PCI, PSP

Executing Crisis: A C-Suite Crisis Leadership Survival Guide
Jo Robertson

Building an Effective Cybersecurity Program, 2nd edition
Tari Schreider

Practicing Forensic Criminology
Kevin Fox Gotham, CPP, and Daniel Bruce Kennedy, CPP

From Sheepdog to the C-Suite*
Kevin Rice and Phil Carlson

Run, Hide, Don't Freeze: Teach your children what to do when faced with danger
Dave Ainsworth, CPP

The Professional Protection Officer: Practical Security Strategies and Emerging Trends, Second Edition
Sandi Davies and Lawrence Fennelly

Chinese Communist Espionage: An Intelligence Primer
Peter Mattis and Matthew Brazil

Interminable: Stories and Steps to Overcoming Life's Obstacles after a Repetitive Cycle of Pain and Loss
Michael L. Henderson

The Handbook of Loss Prevention and Crime Prevention, Sixth Edition
Larry Fennelly

Some processes include written assessments, nonverbal communication, and analysis of verbal cues. The book delves into topics such as varied interview and analysis techniques, preemployment interviewing, and report writing, as well as dealing with angry people, children, and mentally challenged subjects. The authors also provide a summary at the end of each chapter, helping the reader focus on that chapter's crucial points.

The focus and intent of the book is to make the reader more proficient in the interview process, and this book hits the mark. The authors provide case studies to illustrate the methods they mention in the book, and they offer multiple techniques to obtain truth. The search for truth is many times a lengthy process. It is also an extremely important one. This book is a must for the practitioner involved in searching for the truth in today's highly complex work environment.

REVIEWER: *Ernie Van der Leest, CPP, is a retired 28-year veteran law enforcement officer. He has conducted hundreds of interviews and interrogations throughout his career. Van der Leest volunteers on the ASIS Investigations and the Law Enforcement Liaison Councils.*

ASIS
WEBINARS

AUGUST

6 Decoding Enterprise Security Risk Management—A Roadmap for ESRM Program Success

11 Adapting Your Emergency Communication Plan Post-COVID-19 Using Mass Notification

ASIS GLOBAL
EVENTS

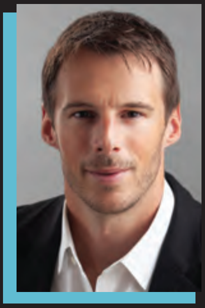
SEPTEMBER

21–25 Global Security Exchange Plus (GSX+)

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

CERTIFICATION PROFILE

ALEXANDER CHOREN, CPP, PSP



"A great résumé will only get you so far."

That's according to Alexander Choren, CPP, PSP, founder and managing director of Rosca Solutions in Atlanta, Georgia, USA—a firm specializing in the protection of critical infrastructure and other irreplaceable assets.

Choren began his career as an electrical engineer providing technology solutions in the world of nuclear security. He felt captivated by the security practice, enjoying the creative approach—in tandem with a thorough understanding—that is required to identify the best solution.

Given his background in engineering, Choren knew he had his work cut out for him as he began his own company to firmly establish his credibility in the security management field.

"As a senior member within the Institute of Electrical and Electronics Engineers (IEEE), I have consistently sought out professional organizations to receive relevant industry information and insights that build value for myself and my clients," he shares. "Project coworkers informed me that ASIS International serves as the cornerstone of the security management profession, so I joined in 2016—mere months after founding my firm."

He set his sights on the Certified Protection Professional (CPP®) and Physical Security Professional (PSP®) certifications to improve his capabilities. He became involved in the ASIS Greater Atlanta Chapter to tap into the collective experience of his local security peers as he prepared to take these exams.

"My ASIS membership has provided multiple outlets for industry engagement and learning that I would not otherwise have had access to," he reflects. "I benefited greatly from local chapter involvement on my way to becoming certified and have become connected with international experts in my field through my involvement in security councils, like the Crime Prevention Community on ASIS Connects."

Following his preparation, Choren passed both the CPP and PSP exams in 2019—both on his first attempt. He has since reaped the benefits.

"Clients, customers, and coworkers need to be assured that you are engaged in security trends and actively involved in a community of other security practitioners," he reasons. "ASIS certification was the most effective opportunity for me to demonstrate my commitment to the security field. My CPP and PSP certifications deliver confidence that I am acting on the latest body of knowledge."

At Rosca Solutions, Choren leads a team of technology-focused engineers and other security-minded professionals to integrate technologies and sculpt new safety regulations for clients around the globe. He makes certification a goal for his team members.

"When someone within our organization attains a certification, it lets me know that this individual prioritizes knowledge expansion and personal growth," he explains. "We reward employees who achieve certification with increased responsibility and greater project visibility."

Over the course of his career, Choren has crafted nuclear security guidelines for an entire nation. He thrives at the intersection of technology and problem solving. The rewarding feeling he experiences from delivering a positive impact for individuals and their communities is the cherry on top of a job well done.

PROFILE BY **STEVEN BARNETT,** ASIS COMMUNICATIONS SPECIALIST

LEGAL REPORT | BY SARA MOSQUEDA

JUDICIAL DECISIONS

PUBLIC HEALTH. A U.S. state supreme court found that Wisconsin's governor overstepped in issuing a month-long extension of stay-at-home orders in response to the coronavirus pandemic. Originally issued in March, the state's stay-at-home order closed schools and nonessential businesses; it was extended to the end of May by Wisconsin Health Secretary Andrea Palm.

In a 4-3 ruling, the Wisconsin Supreme Court judges overruled Governor Tony Evers' decision to keep the state closed, limit the size of gatherings, bar nonessential travel, and keep businesses—including restaurants and bars—shut down. The decision reopened the state, although it also kept the language that closed schools and allowed local governments to levy their own restrictions.

"Palm's order confining all people to their homes, forbidding travel, and closing business exceeded the statutory authority of [Wisconsin]," according to the ruling. (*Wisconsin Legislature v. Secretary-Designee Andrea Palm, et al.,* Supreme Court of Wisconsin, Case No. 2020AP765, 2020)

CORRUPTION. A U.S. appeals court rejected U.S. President Donald Trump's attempt to end a lawsuit that alleged he violated constitutional anti-corruption provisions as owner of a hotel in Washington, D.C., while also in office.

The lawsuit, filed in 2019 by the attorneys general of Maryland and the District of Columbia, claims that the U.S. Constitution's emoluments clause prohibits a president from accepting foreign governments' gifts or payments without the approval of Congress. The clause questions the legality of Trump's opening the Trump International Hotel in Washington, D.C., just before being elected in 2016.

Some foreign and U.S. state officials have chosen to stay at the hotel or use it as an event space.

The case will return to a federal court in Maryland. Trump's lawyer, Jay Sekulow, is expected to continue to appeal decision. (*District of Columbia v. Donald Trump,* U.S. Court of Appeals for the Fourth Circuit, No. 8:17-cv-01596-PJM, 2020)

LEGISLATION

Cambodia

MONEY LAUNDERING. Two draft laws aimed at addressing money laundering, terrorism financing, and the proliferation of weapons of mass destruction were approved by Cambodian cabinet officials.

The bill on anti-money laundering and counter-terrorist financing aims to control, prevent, suppress, and ultimately eliminate such crimes.

The other draft law proposes greater control over and in fighting against providing funds, financing, or support for the proliferation of weapons of mass destruction, including the export or transportation of materials for such weapons.

The bills will need to be approved by Cambodia's National Assembly, then reviewed by the Senate, and finally submitted to and approved by King Norodom Sihamoni before going into effect.

PHOTOS BY ISTOCK

LEGAL HIGHLIGHTS

COURT CASES

ISSUE: Election interference
CASE: *United States v. McMahon*
VENUE: U.S. Dist. Ct. for the West. Dist. of Virginia
STATUS: McMahon pled guilty
SIGNIFICANCE: Daniel McMahon pled guilty to threatening a Black candidate for Charlottesville City Council because of his race.

ISSUE: Discrimination
CASE: *EEOC v. Faurecia Automotive Seating*
VENUE: U.S. Dist. Ct. for the N. Dist. of Mississippi
STATUS: Settled
SIGNIFICANCE: Faurecia will pay $825,000 to settle charges that it based hiring decisions on applicants' prior sick leave use.

United States

HEALTH PRIVACY. U.S. legislators introduced a bill proposing stronger privacy and data and security rights around Americans' health information.

The Public Health Emergency Privacy Act (PHEPA), spearheaded by U.S. Senators Richard Blumenthal (D-CT) and Mark Warner (D-VA), would impose temporary rules concerning the collection, use, and disclosure of emergency health data.

The act would only apply to certain data that was used to mitigate the spread of the COVID-19 pandemic. Such data—which would be used to track, screen, monitor, or contact trace in response to the coronavirus—includes geolocation data, proximity information, and demographic records. Organizations would be limited to only collecting, using, or releasing that information when necessary for health purposes.

The bill calls for the creation and use of data security policies, practices, and procedures; securing explicit consent before collecting, using, or disclosing the data; informing data subjects how the information would be used prior to collection; publishing a public report every 90 days on the number and scope of data subjects; and destroying the data 60 days after the public health emergency ends.

The COVID-19 Consumer Data Protection Act, which was introduced by Republican backers in April, is largely similar to the PHEPA.

FOR MORE INFORMATION:

CAPITOL SWITCHBOARD (INFORMATION):
202.224.3121

LEGISLATIVE STATUS OFFICE (STATUS OF BILLS):
202.225.1772

To see the full text of selected regulations, bills, and reports, visit ***sm.asisonline.org****.*

REGULATIONS

Germany

PRIVACY. German federal agencies were ordered not to use WhatsApp due to concerns that it provides data to its parent company, Facebook.

Data Privacy Commissioner Ulrich Kelber prohibited any use of the app for federal ministries and institutions, claiming that even sending messages would deliver metadata—such as IP addresses and geolocations—to WhatsApp, which in turn feeds a larger collection of personal data.

A WhatsApp spokesperson said that the company does not forward user data to Facebook, and that a default setting encrypts messages—meaning that only the sender and receiver can read them.

European Union

CYBERSECURITY. The Council of the European Union extended its cyber sanctions regime framework for another year, until 18 May 2021.

The framework allows the EU to maintain its ability to levy sanctions against cyber attackers who target EU nations, imposing "targeted restrictive measures" on those who threaten the EU or an EU nation. Such sanctions can include a ban on persons travelling to the EU, freezing persons' or entities' assets, and banning EU residents and organizations from financing those who have been sanctioned.

The cyber sanctions were originally adopted in May 2019 as part of a larger, years-long effort to increase the EU's resilience and response to "cyber threats and malicious cyber activities in order to safeguard European security and interests," according to a statement by the council.

INTERNATIONAL LEGISLATION

United Kingdom

Organ donors. England shifted its organ donation system from an "opt in" system to a default enrollment program, meaning that all adults in the country will automatically be registered as organ donors in the event of their death unless they record a differing decision.

Under Max and Keira's Law (or the Organ Donation Act), effective 20 May 2020, adults who do not want to be organ donors must record their donation decision on the UK's National Health Service Organ Donor Register.

Certain groups are excluded from the law, including persons under the age of 18; persons lacking sufficient mental capacity to understand the changes to the law; tourists or people not living in the country voluntarily; and anyone who lived in England for less than one year before his or her death.

LEGISLATION

ISSUE: Agriculture safety
BILL: P.L. 116-122
VENUE: U.S. Executive Branch
STATUS: Enacted
SIGNIFICANCE: Increases the number of U.S. Customs and Border Protection agriculture specialists and support staff.

ISSUE: Retaliation
BILL: HB 984
VENUE: Virginia
STATUS: Enacted
SIGNIFICANCE: Allows individuals to file civil actions against employers for failing to classify them as employees.

United States

SUPPLY CHAIN. U.S. President Donald Trump used his powers under the Defense Production Act to order slaughterhouses and meat packing plants to remain open during the COVID-19 pandemic.

Although several U.S. states had issued shelter-at-home orders at the time, Trump said in the 28 April 2020 order, "Such closures threaten the continued functioning of the national meat and poultry supply chain, undermining critical infrastructure during the national emergency."

> ***Such closures threaten the continued functioning of the national meat and poultry supply chain.***

The administration said it would provide additional protective equipment and guidance, although whether that occurred remained unconfirmed by the time of this article's publishing deadline. The order applied to plants that are part of the beef, chicken, pork, and egg supply chains.

The Defense Production Act grants the U.S. federal government the ability to direct industrial production during times of crisis.

Unions criticized the order, claiming that many slaughterhouse facilities or meat packing plants were not appropriately equipped to protect workers. ▨

This column should not be construed as legal or legislative advice.

ELSEWHERE IN THE COURTS

TAX FRAUD

Dr. Xiao-Jiang Li, a former professor at Emory University in Atlanta, Georgia, was sentenced to one year of probation for filing a false tax return. Along with his position at the university, Li was also a participant in the Chinese Thousand Talents Program and worked overseas at Chinese universities—information and income he did not include on his federal tax returns. Li actively worked as a researcher for the Chinese government's talent recruitment program from 2012 to 2018, and he earned at least $500,000 from the position. Li was ordered to pay $35,089 in restitution and to file lawful income tax returns for 2012 through 2018 within the first two months of his probation. (*United States v. Li*, U.S. District Court for the Northern District of Georgia, No. 1:19-mj-01007-RDC, 2020)

SEXUAL ABUSE

A U.S. district judge sentenced Douglas S. Groover to 60 years in prison for producing hundreds of videos and images of himself while sexually abusing a child. The sentencing also included a lifetime term of supervised release and a restitution of $53,000. Groover pleaded guilty to two counts of production of child pornography in February 2020, and he admitted to abusing at least two other minors and keeping a collection of child pornography. (*United States of America v. Douglas Stephen Groover*, U.S. District Court for the Northern District of Texas, No. 6:19-cr-00039-H-BU, 2020)

DISCRIMINATION

FedEx Ground Package System, Inc., will pay $3.3 million to settle a companywide disability discrimination suit. The lawsuit, filed by the U.S. Equal Employment Opportunity Commission (EEOC) in 2014, alleges that the company denied deaf and hard-of-hearing package handlers reasonable accommodations, as well as discriminating against this class as applicants to package handler positions. As part of the settlement, FedEx Ground will also provide programmatic relief, including access to live and video remote American Sign Language interpreting, captioned videos, and scanning equipment with cues like vibrations. FedEx was also ordered to take additional measures to protect the safety of its deaf and hard-of-hearing package handlers, such as providing warning lights on motorized equipment and personal emergency notification devices. (*EEOC v. FedEx Ground Package System, Inc.*, U.S. District Court for the Western District of Pennsylvania, No. 2:15-cv-00256, 2020)

LEGAL HIGH-LIGHTS

LEGISLATION

ISSUE: Pandemic response
BILL: P.L. 116-139
VENUE: U.S. Executive Branch
STATUS: Enacted
SIGNIFICANCE: Provides funding for small business loans, healthcare providers, and COVID-19 testing.

ISSUE: Sick leave
BILL: New York Labor Law amendment
VENUE: New York
STATUS: Enacted
SIGNIFICANCE: Requires New York employers to provide paid or unpaid sick leave to their employees.

PHOTO COURTESY OF AMG

MOTORWAY SURVEILLANCE

Working with Juniper Networks, AMG Systems helped digitize the traffic monitoring system for the hard shoulder bus lanes on two main highways and motorways in Belfast, Ireland. As part of a Northern Ireland Department for Infrastructure extension project on the M1 and M2 motorways, the installed IP-based surveillance system will transmit high-grade images in real-time back to the city's Traffic Information and Control Centre (TICC) and its traffic management teams, all aimed at improving the motorways' efficiency, security, and reliabilty. AMG connected the newly upgraded IP cameras onto the existing fiber network and the new monitoring equipment, providing the TICC with nine switches on the M1 fiber network, 15 switches for the M2, and four switches at the TICC control room.

MERGERS & MOVES

WESCO International, Inc. ⇆ Anixter International Inc.

The merger created a global business-to-business distribution and supply chain solutions company.

FON Advisors, LLC ⇆ FON Corporate Finance, LLC

FON Corporate will center on providing professional, strategic, and financial advisory services, focusing on the aerospace, defense, and government industry.

Sealing Technologies Inc ⇆ Quark Security Inc.

With the acquisition, Sealing Tech provides additional mobile, cross-domain, and critical infrastructure solutions to its clients.

Raytheon Company ⇆ United Technologies Corporation

Raytheon Technology Corporation, formerly United, provides a portfolio of high technology products and services to the building and aerospace industries.

AWARD

The Security Industry Association's Open Supervised Device Protocol standard was approved by the International Electrotechnical Commission's technical committee on alarm and electronic security systems as an international standard.

CONTRACT

Teleste Corporation will supply information displays and passenger information system to the Braunschweig Transit Authority in Germany.

ANNOUNCEMENT

Hanwha Techwin America announced a new occupancy monitoring system and mask detection analytic to ensure occupancy levels stay below preset limits and masks are worn as businesses reopen.

PARTNERSHIPS

WORKFORCE MANAGEMENT

TrackTik Software, Inc., is working with **Badger Technologies'** PatrolBot autonomous robot for security guard tour scheduling, real-time checkpoint logging, and more.

INTERNET OF THINGS

Keyfactor and **PrimeKey** partnered to enable a simplified and automated public key infrastructure for large-scale enterprise and Internet of Things (IoT) deployments.

DIGITAL ASSETS

Aon UK Ltd and **GK8** partnered to allow GK8's clients to benefit from up to $500 million in insurance coverage of digital assets.

NEW PRODUCTS

Included in this month's solutions are video encoders, surveillance cameras, fencing brackets, and more.

HD VIDEO ENCODER | #801

Johnson Controls introduced the Tyco HD Encoder, a solution allowing for high definition and standard definition analog cameras to function within an evolving IP infrastructure. Available in one- and four-channel options, the encoder allows users in networked environments to retain HD and SD cameras, plus the option of adding IP cameras over time while utilizing existing analog infrastructure. The encoder's hardware adapts to analog video to be sent over IP networks, helping CCTV systems upgrade to a more modern IP video surveillance organization.

jci.com

MOUNTING BRACKET | #802

D&D Technologies introduced three new sizes of its half bolt-on line: a 4-inch Half Bolt-on with aluminum, 4-inch Half Bolt-on with steel/aluminum combo, and 6-inch Half Bolt-on with aluminum. These new brackets, suitable for 4- and 6-foot fenceposts, are designed to reduce post flexing. The wider hinges on the Shut It mounts enable anchor points to be positioned at the sides instead of the center of the fence post, increasing stability and decreasing flexing. The brackets can handle gate loads of up to 1,000 pounds, and their nearly frictionless operation allows for long-term dependability in all weather conditions.

ddtech.com

MINI PCS | #803

OnLogic announced the availability of their line of mini PCs. Powered by AMD Ryzen Embedded processors, the units can be used in manufacturing, automation, transportation, digital media, medical, and other IoT and Industry 4.0 applications. The ML100G-40, MC510-40, MK400-40, and upcoming MC850-40 offer various compact solutions, from passive cooling to digital signage and workstation applications to dedicated graphics card support with room for 7 GPUs.

onlogic.com

CABLE MANAGEMENT | #804

Platinum Tools announced the launch of its new high performance hybrid J-Hook line, available in four colors and four sizes in standard and batwing configurations. Designed to support modern network cable installations, the hooks are built with steel J-Hooks over-molded with Plenum-rated polypropylene, allowing for cables to easily slide. The Snap-Lock retainer can firmly secure cables. The hooks also feature a smooth, radiused 2-inch wide base with no pressure points, and are UL listed, RoHS, and TIA compliant. The hook's bend radius of more than 3.5 inches prevents deformation to the cables.

platinumtools.com

MULTI-DIRECTIONAL CAMERAS | #805

Hanwha Techwin America announced the availability of its latest multi-sensor cameras, which feature motorized varifocal lenses for control of focal length, angle of view, and zoom for each direction. Each sensor supports remote pan, tilt, rotate, and zoom control for efficient installation and easy adjustment. The 2MP PNM-9084RQZ and 5MP PNM-9085RQZ feature built-in IR illumination for each sensor, while the 2MP PNM-9084QZ is a cost-efficient four channel PTRZ camera.

hanwhasecurity.com

REQUEST DETAILED PRODUCT INFORMATION THROUGH OUR MONTHLY E-RESPONSE, VISIT HTTP://SECURITYMGMT.HOTIMS.COM, OR USE YOUR SMART PHONE 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 #
05	ADT Commercial	11
02	Axis Communications	04
14	Garrett Metal Detectors	35
03	HID Global	06
17	Mission 500	47
20	Alarm Lock/Napco	68
06	Paladin Security	13
11	Par-Kut International	25
01	SecurAmerica, LLC	02-03
09	Special Response	22

ADVERTISERS ONLINE

ADT Commercial
www.adtcommercial.com

Axis Communications
www.axis-communications.com

Garrett Metal Detectors
www.garrett.com

HID Global
www.hidglobal.com/signo

Mission 500
www.mission500.org

NAPCO / Alarm Lock
www.alarmlock.com

Paladin Security
www.palamerican.com

Par-Kut International
www.parkut.com

SecurAmerica, LLC
www.securamericallc.com

Special Response
www.specialresponse.com

GETTING TO KNOW

LISA OLIVERI, CPP, IS DIRECTOR OF GLOBAL SAFETY AND SECURITY FOR THE EDUCATION DEVELOPMENT CENTER, A GLOBAL NONPROFIT ORGANIZATION FOCUSED ON IMPROVING EDUCATION, PROMOTING HEALTH, AND EXPANDING ECONOMIC OPPORTUNITY. OLIVERI, VICE CHAIR OF THE ASIS INTERNATIONAL CSO CENTER, SHARES CAREER ADVICE AND INSPIRATION.

Q. What does ASIS mean to you?
A. The first words that come to mind are community, education, and leadership. I am continuously learning and thinking about security and the future of the industry in different ways, thanks to the expertise and innovation within the ASIS community.

Q. What is the best advice you've gotten regarding your career?
A. Volunteer for opportunities that will help you develop professionally, be authentic while expanding your network, and don't undervalue yourself or your experience.

Q. Tell us about a mentor who inspired you.
A. I connected with Angela Scalpello, a C-suite advisor and executive coach, at the CSO Summit in 2018. I was immediately drawn to Angela's approach to strategic thinking, storytelling of lessons learned, and creation of a safe space for people to be honest about their skill gaps and their potential to drive change and transformation.

Q. What book has inspired you?
A. I recently read Simon Sinek's *Leaders Eat Last.* His perspective on successful leadership and the impact of creating an environment where people feel like they and their work matter is inspirational and applicable to any sector.

Q. If you could go back in time and give yourself some advice, what would it be?
A. Become proficient in as many languages as you can and try not to agonize over how to articulate something perfectly if it means you'll lose an opportunity to share your perspective and ideas.

listen to

SECURITY

MANAGEMENT

S M PODCAST

DID YOU **HEAR?**

Security Management Highlights is a monthly podcast that brings the security professional expert interviews and information on the most critical industry topics. Each month, host **Chuck Harold** interviews thought leaders and industry professionals, as well as editors from the magazine.

Available on iTunes

SOUNDCLOUD

Apple and the Apple logo are trademarks of Apple Inc., registered in the U.S. and other countries. iTunes Music Store is a service mark of Apple.

SoundCloud logo is a registered trademark of SoundCloud Limited.

Lock Down Peace of Mind

ArchiTech® Locks with LocDown® Keyfobs & Strobe

- **ArchiTech Wireless Access Control LocDown® Locks,** standalone locks or locks networked campus-wide via 802.11 or Ethernet – Enterprise security integration, too
- **Keyfob-Activated Lockdown & bright flashing strobe indicator** on inside door gives security control & peace of mind to occupants
- **Lock down One Door or a Global Lock Group** in seconds from any keyfob on the system (each with programmable access, lock- and unlock-privileges)
- **Customizable, sleek minimalist look,** choice of levers, multi-technology access ID readers, in various colors, shapes & architectural finishes
- **Quickly retrofits any standard door lock;** cylindrical models feature easy surface mount electronics & years of battery life (AAs), on all doors
- **Keyless access for up to 5000 users,** w/ 500 Scheduled Events & 36,000 Event Log. Integration w/

connected Software House   Lenel   CA4K

Locdown Keyfobs - Staffers lock down one, or all networked doors in seconds

Inside in Emergency

Lockdown Flashing Strobe *-Highly visible across the room, e.g., while sheltering in place*

ALARM LOCK

From the makers of Trilogy® – The #1 Locks in their Class

Schedule a Free Certified SAVI School Security Audit Onsite

1.800.ALA.LOCK • salesinfo@alarmlock.com • **www.alarmlock.com**

ArchiTech Networx N90L LocDown Lock, shown above, with silver oval HID Prox ID Reader & American Lever in US26D. ArchiTech, Trilogy, & LocDown are trademarks of NAPCO Security Technologies/Alarm Lock Systems Division. All others are trademarks of their respective companies.

For product info #20 securitymgmt.hotims.com