SECURITY
MANAGEMENT
SEPTEMBER 2020
A PUBLICATION OF ASIS INTERNATIONAL

Issue & Beyond

- ***National Security***
  How can forces better retain female servicemembers?
- ***Cybersecurity***
  Transparency around privacy boosts consumer trust.

×42
SECURITY AWARENESS

×48
DRUG DIVERSION

×56
REMOTE HIRING

×34 PREDICTING PROTESTS

Hanwha Techwin

It begins with image quality…

- 4K resolution produces clear and vivid images
- Extreme WDR allows detailed objects to be seen clearly even in strong backlight conditions
- Enhanced noise reduction identifies objects faster and easier, even in low-light environments
- Digital Image Stabilization reduces the motion blur caused by wind or vibration
- Lens Distortion Correction eliminates the distortion created by conventional camera designs with wide-angle lenses

Protected by total cybersecurity, built-in from the ground up…

- Secure by Default, Hanwha Techwin's cybersecurity policy, embeds unique certificates into all products during development and manufacturing
- A unique cybersecurity policy that satisfies stringent UL CAP standards

Delivering an unprecedented level of user convenience…

- Wisenet 7 X series PLUS modular dome-style camera design reduces installation time and cost
- OSD vector graphics deliver powerful camera identification and branding capabilities

And operational efficiency…

- WiseStream II with H.265 compression technology achieves up to a 99% reduction in bandwidth and storage costs
- USB and mobile app support, dual micro SD card slots

For an end-to-end intelligent video surveillance solution.

- License-free video and audio analytics for enhanced monitoring, forensic review, sound classification and audio event playback
- Artificial Intelligence algorithms support automatic or manual object tracking

© 2020 Hanwha Techwin America, Inc.

WISENET 7

Cyber Security

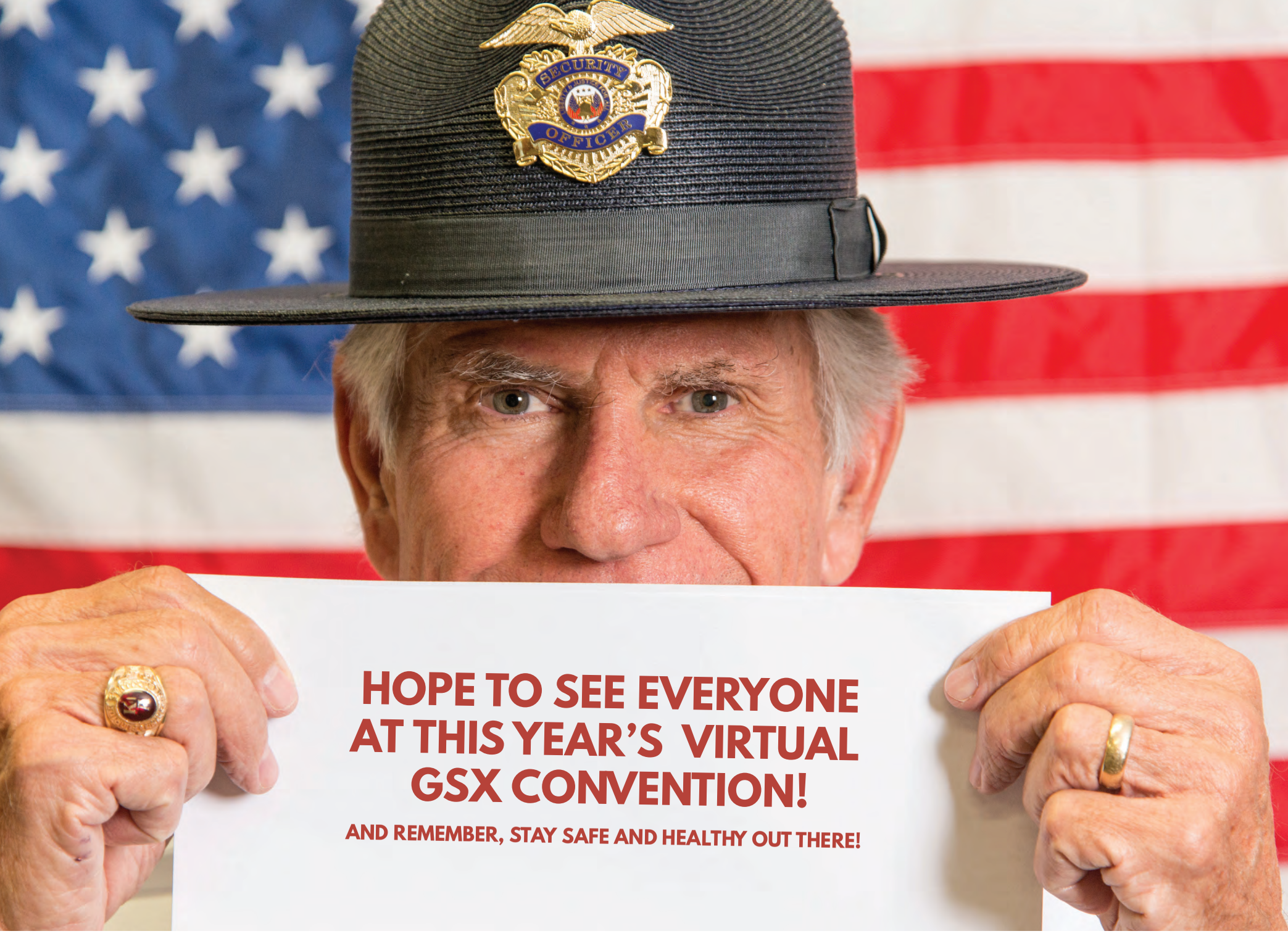
extreme WDR

System on Chip (SoC).
Excellence Through Innovation.

At the heart of Hanwha Techwin's new product development is the Wisenet 7 System on Chip (SoC). Designed in-house and built in Korea, Wisenet 7 is our most technology-intensive and feature-rich chipset. From its enhanced image quality and total cybersecurity to unprecedented user convenience and operational efficiency, Wisenet 7 delivers end-to-end intelligent video surveillance capabilities today…and tomorrow.

For product info #1 securitymgmt.hotims.com

HanwhaSecurity.com


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.

For product info #2 securitymgmt.hotims.com

Smarter surveillance for safe & secure hospitals.

With evolving healthcare demands, protecting patients, providers, and PPE is more challenging than ever.

By utilizing intelligent video, audio, analytics, and access control, you can supply security and clinical teams with the tools they need to provide a safer and more secure healing environment. See what's possible with innovative Axis technologies to improve overall security, patient care, and business efficiencies.

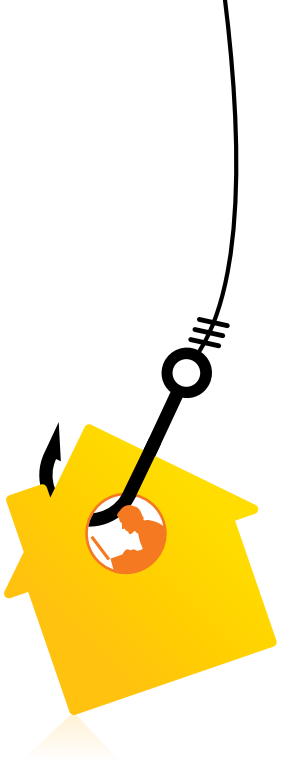
Visit www.axis.com/healthcare

AXIS® COMMUNICATIONS

For product info #3 securitymgmt.hotims.com

CONTENTS

NOTABLE



"Home networks are some of the most hostile networks on the planet."

Despite a widespread shift to remote work, consumers' concerns over cybersecurity issues are lagging, says Mathew Newfield at Unisys. PAGE 18

77

The percentage of Americans who say sexual harassment is a major obstacle to equal rights for women, according to a recent poll. PAGE 21

PHOTOS BY ISTOCK, ILLUSTRATIONS BY *SECURITY MANAGEMENT*

"If someone cannot manage a Zoom or Webex interview, how effectively can they be expected to use a mobile device complete with accountability and reporting software?"

Chris Stuart explains why remote hiring processes might extend beyond the pandemic. PAGE 62

The year-over-year increase in U.S. opioid overdose fatalities for the first four months of 2020, largely attributed to the impacts of quarantines, lockdowns, and economic uncertainties on addiction. PAGE 50

"We are living in an age of mass protest."

The Center for Strategic and International Studies assessed recent civil unrest risks, which are likely to persist long into the 2020s. PAGE 34

BPA WORLDWIDE

Security Management (ISSN 0145-9406) Volume 64, Number 9, 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. Copyright © 2020 ASIS International, Inc. This information is protected by copyright and trade mark laws under U.S. and International law. No part of this work may be reproduced without the written permission of ASIS International. 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.

SM

MORE CONTROL, LESS CONTACT

50% Off First-Year Subscription of Mobile IDs

LEADING AN ECONOMIC RECOVERY REQUIRES A FASTER AND SAFER RETURN TO THE WORKPLACE

As people return to their workplace, they will expect to see more rigorous cleaning and disinfection routines, frequent hand washing and sanitizing, minimal use of shared surfaces, and **increased use of touchless access control technologies.**

REDUCE ANXIETY AND ENABLE A SAFE RETURN WITH 50% OFF YOUR FIRST-YEAR SUBSCRIPTION OF MOBILE IDS.

- Minimum order increment of 20 Mobile IDs
- Promotion ends December 31, 2020 (not valid for renewals)

Learn More or Request a Free Consultation

hidglobal.com/mobile50

HID

For product info #4 securitymgmt.hotims.com

© 2020 HID Global Corporation/ASSA ABLOY AB. All rights reserved. HID, HID Global, the HID Blue Brick logo, the Chain Design, Identrust an HydrantID are trademarks or registered trademarks of HID Global or its licensor(s)/supplier(s) in the US and other countries and may not be used without permission. All other trademarks, service marks, and product or service names are trademarks or registered trademarks of their respective owners.
2020-07-10-pacs-promo-half-off-mobile-ids-ad-en

CONTENTS

FEATURES

SEPTEMBER 2020

ASIS INTERNATIONAL
Advancing Security Worldwide®

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

Nancy Green, FASAE, CAE
chief global learning and strategy officer
Nancy.Green@asisonline.org

Nello Caramat
publisher
Nello.Caramat@asisonline.org

BUSINESS OFFICES
1625 Prince Street
Alexandria, VA 22314

703.519.6200
fax 703.519.6299

MEDIA SALES
Charlotte Lane
media sales manager

703.518.1510
Charlotte.Lane@asisonline.org

On the Cover:
Illustration by Daniel Hertzberg

COVER STORY

34

SEEDS OF DISRUPTION

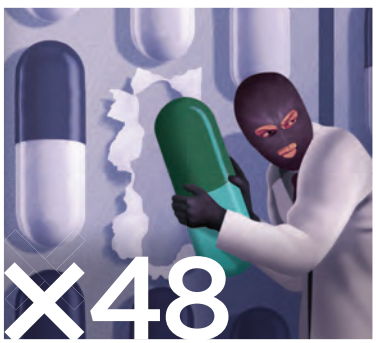
The world is entering a decade of rage, unrest, and shifting geopolitical sands. Security leaders need to understand the factors behind mass protests to accurately predict them and mitigate their effects.

By Michael Center and Dieter Arendt

SECURITY AWARENESS

A CONVERGED CAMPAIGN

With a converged security team, Mastercard is taking a unified approach to addressing risks and educating its workforce to reduce threats.
By Megan Gates



DRUG DIVERSION

BITTER PILLS

As drug diversion temptations rise, healthcare facilities face multitiered loss prevention challenges stemming from an opioid epidemic and the effects of the COVID-19 pandemic.
By Mark Giuffre, CPP

SECURITY SERVICES

VIRTUAL VETTING

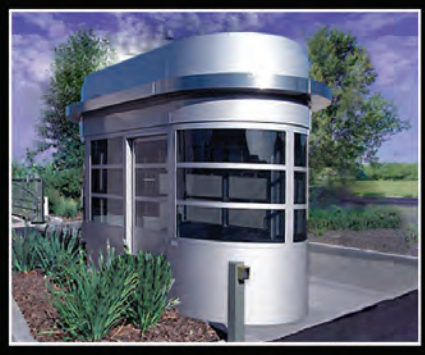
Emerging technology, changing client demands, and multigenerational staff management were already changing the hiring process for security staffing companies. Then COVID-19 came along.
By Chris Stuart

SM

"NO ONE MAKES A BETTER BOOTH THAN B.I.G."

LIMITLESS PREFABRICATED BOOTHS

Visit us at BigBooth.com to find the options that meet your demanding security or site-specific requirements.



Quality Workmanship

"When I visited the B.I.G. facility, I saw that it was a very well run and lean ship. Quality workmanship was obvious from the moment I walked in. Everybody worked as a team to secure our nuclear power facility. We're very pleased with B.I.G.'s performance—they made a big difference."

Mission Critical Security Specialist

WWW.BIGBOOTH.COM

Ph. 626-448-1449 • Toll Free 1-800-669-1449

For product info #5 securitymgmt.hotims.com

SEPTEMBER 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 MICHAEL AUSTIN

X30

CYBERSECURITY
When it comes to a business's reputation, consumer trust and privacy are increasingly intertwined. Increased transparency about security policies, procedures, and problems can build bridges.
By Megan Gates

12
CONTRIBUTING AUTHORS

14
SM DIGITAL

16
EDITOR'S NOTE
How to connect.

17
COVID-19: SECURITY RESOURCES

18
NEWS & TRENDS
Awareness campaigns go virtual.
By Claire Meyer

22
NATIONAL SECURITY
Militaries seek methods to retain female servicemembers.
By Mark Tarallo

26
CASE STUDY
An access control upgrade empowers school staff to initiate lockdowns.
By Megan Gates

64
GSX+ PRODUCT SHOWCASE

72
ASIS NEWS
GSX+ unveils its education lineup.

73
ASIS GLOBAL BOARD OF DIRECTORS

76
LEGAL REPORT
The U.S. Supreme Court ruled that LGBTQ employees are protected from sexual orientation discrimination.
By Sara Mosqueda

79
INDUSTRY NEWS
By Sara Mosqueda

80
MARKETPLACE

81
ADVERTISER INDEX

84
THE LIST
Five rules for crisis leadership.
By Jo Robertson

CHECK OUT MORE ONLINE
at *securitymanagement.com*

SM

CONTRIBUTING *AUTHORS*

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 vice chair of the ASIS International Professional Development Council and the vice chair for the ASIS Council on Global Terrorism, Political Instability, and International Crime. He has also served on the Academic and Training Programs Council.

"Seeds of Disruption"
PAGE 34

DIETER ARENDT
SECURITY ANALYST
SOUTH AFRICAN RESERVE BANK

Dieter Arendt has 27 years of experience in law enforcement and critical infrastructure security. He is responsible for security assessments, investigations, and project security management for the South African Reserve Bank (SARB) Group. He has a B.A. in international politics, political science, and African politics, holds a diploma in security management, and is currently studying for the CPP certification.

Arendt serves on the ASIS Global Terrorism, Political Instability, and International Crime Council. He has participated in various South African Bureau of Standards technical committees and the Central Banks Heads of Security: Good Guidance Group (Critical Infrastructure).

"Seeds of Disruption"
PAGE 34

MARK GIUFFRE, CPP
DIRECTOR
HILLARD HEINTZE

Mark Giuffre, CPP, CFE (Certified Fraud Examiner), CAMS (Certified Anti-Money Laundering Specialist), is a globally recognized expert in narcotics control, investigations, and opioids, with 30 years of service as a special agent with the U.S. Drug Enforcement Administration. He has instructed investigators, prosecutors, and judges, and testified as an expert witness. He teaches classes for the International Narcotics Interdiction Association.

At Hillard Heintze, a Jensen Hughes Company, Giuffre manages investigations, security, and law enforcement consulting projects. He is a member of ASIS, the Illinois Security Professionals Association, the Association of Threat Assessment Professionals, and the Association of Federal Narcotics Agents.

"Bitter Pills"
PAGE 48

CHRIS STUART
VICE PRESIDENT
TOP GUARD SECURITY

Chris Stuart is vice president of Top Guard Security, which is headquartered in Virginia and employs 1,100 security officers. He has served on several ASIS councils and has written or been interviewed for multiple *Security Management* articles.

Stuart has been a member of the Commonwealth of Virginia's Private Security Services Advisory Board, is past president of the Virginia Security Association, and is chairman of the Virginia Maritime Association's Port Protection and Emergency Response Committee. Stuart attended Old Dominion University for his undergraduate and graduate degrees. He also holds a Career Certificate in Acquisitions and Procurement from Thomas Nelson Community College.

"Virtual Vetting"
PAGE 56

AMICO SECURITY PERIMETER SYSTEMS DELIVER THE PROVEN SOLUTIONS FOR DATA CENTERS TO PROVIDE A FORMIDABLE BARRIER TO INTRUSION.

FULL RANGE OF PERIMETER SOLUTIONS WITH A WIDE ARRAY OF MEDIUM TO HIGH SECURITY DESIGNS

- Anti-climb, anti-cut, ballistic, visual screening
- ANC non conductive designs
- Ability to upgrade an existing chain link fence

CRASH RATED ANTI-VEHICULAR EQUIPMENT

- Cable Systems
- Full array of Crash Gates and Crash Arms
- Full offering of fixed, removable, shallow and retractable Bollards
- Wedge Barriers

Perimeter Fence Solutions

AMIGUARD® 9000 Series Vehicle Barriers

AMICO SECURITY®

amicosecurity.com/aj/ 855-552-6426

info@amicosecurity.com • www.linkedin.com/company/amicosecurity

For product info #6 securitymgmt.hotims.com

SM DIGITAL

TOP TWEET

While classes moved online and most students went home, Yale researchers carried on their critical research into COVID-19. Here's how campus security is monitoring access to campus to help researchers safely do their jobs.

TOP POST

Cathy Lanier, senior vice president of security for the NFL, shares how the league is addressing the coronavirus and security challenges for the 2020 season.

COMMENTS

"Very interesting and useful information for business travelers." —Raúl Mejía, CPP, security consultant, RM Consulting, commenting on the *Security Management* article "Four Travel Safety Tips."

CURRENT PODCASTS

School security professionals need to prepare to address student anxiety and behavioral challenges, according to Dr. Franci Crepeau-Hobson and Paul Timm, PSP. Also, learn how to apply contextual intelligence to decision making and the value of certification.

SM ONLINE

GENDER EQUALITY

Sexual harassment is a major obstacle to equal rights for women, according to 77 percent of U.S. adults surveyed by the Pew Research Center.

FEMALE SERVICEMEMBERS

Root causes behind low female servicemember retention include poor leadership, a scarcity of female role models, and perceived gender bias, a RAND Corporation report found.

SECURITY AWARENESS

Approximately 40 percent of global consumers said they were seriously concerned about scams or data breaches while working remotely, the *2020 Unisys Security Index* said.

CONVERGENCE

Roughly 25 percent of organizations in certain parts of the world have converged their physical and cybersecurity teams, according to *The State of Security Convergence in the United States, Europe, and India* by the ASIS Foundation.

DISCRIMINATION

The U.S. Supreme Court ruled that the Civil Rights Act of 1964 protects gay and transgender workers from workplace discrimination.

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

TRENDING ARTICLES

1 **RISK MANAGEMENT**
An Unfair Advantage: Confronting Organized Intellectual Property Theft
By Megan Gates

2 **PHYSICAL SECURITY**
Guard Training Programs: A Development Guide
By Glen Kitteringham, CPP

3 **CASE STUDY**
How Yale Is Using Analytics to Monitor Campus Access
By Megan Gates

You're working 6 feet apart. We're working around the world.

As social distancing changes the way we live and work, G4S can help. Whether you need to secure an empty facility or building, manage the flow of visitors and employees to your office, or need the additional support of security officers, we are committed to working closely with you.

Your trusted security advisor. | 888-645-8645 | www.G4S.us

RISK CONSULTING SOFTWARE & TECHNOLOGY SYSTEMS INTEGRATION SECURITY PERSONNEL

© 2020 G4S. All Rights Reserved.

Editor-in-Chief
TERESA ANDERSON

COMMUNITY

Loneliness is the pain of disconnection, according to Dr. Vivek H. Murthy, former surgeon general of the United States. What humans describe as feeling lonely is not about being alone, it's about being removed, disconnected from other people and what matters to us, Murthy writes in his new book *Together: The Healing Power of Human Connection in a Sometimes Lonely World*. "What matters is not the quantity or frequency of social contact but the quality of our connections and how we feel about them."

Even when we are alone and relaxing, our brains are primed and ready for social interaction. "Even if we don't realize it—even if we think of ourselves as profoundly introverted or task-oriented—we spend most of our time thinking about other people," Murthy notes.

For example, neuroscientists have found that the medial prefrontal cortex is active during what is called self-processing, when we are thinking about ourselves—our preferences, our hobbies, our personal decisions. Scientists theorized that this part of the brain should dim when we focus on others, but the opposite happens. "When we're engaged with others, activity in this supposedly self-centered region accelerates," writes Murthy. "So we evolved to have brains that are wired to seek connection, to focus our thoughts on other people, and to define ourselves by the people around us."

Murthy adds that disconnection is a challenge with many layers. For example, researchers have identified three dimensions of loneliness: intimate—longing for a close friend or partner; relational—longing for social companionship; and collective—a "hunger for a network or community of people who share your sense of purpose and interests."

Collective loneliness confronts many security professionals as the pandemic prevents them from connecting with their peers in the industry, those who form a community of shared interest and purpose. Combating this disconnect is the mission of GSX+, a virtual experience taking place 21–25 September that is designed to foster communication, connection, and education in the security industry.

Attendees can access more than 80 education sessions in live and on-demand formats (see page 72). Keynote presenters such as General Stanley McChrystal, cybersecurity expert Keren Elazari, and author Max Brooks will offer insight into navigating the variety of challenges faced by security professionals.

The GSX+ platform puts the focus on connecting with other security professionals and organizations of interest through an advanced chat function, networking activities, speaker Q&A sessions, and one-on-one meetings. GSX+ attendees can learn more about ASIS certifications, membership, standards and guidelines, and security careers by visiting the Hub.

Since COVID-19 emerged, personal connection seems more remote than ever. The GSX+ experience offers a respite from collective loneliness, a way to learn from and connect to your community. Register today at *gsx.org*.

COVID-19: SECURITY RESOURCES

The Pandemic Diaries: Tracking COVID-19 Responses Across Industries

To help security professionals benchmark and learn from each other, the ASIS Foundation has been sharing case studies that illustrate security's response to the COVID-19 pandemic. A group of security executives across the globe representing different industries shared their stories in the early phases of the coronavirus pandemic, and the ASIS Foundation has checked in with them throughout the crisis to track their response and recovery efforts.

Recovery Goes Granular at Global Bank: A Canada-based global financial firm is taking a pragmatic, case-by-case approach to reopenings, considering local government mandates, staff opinions, and bank management's own observations.

Furniture Retailer Maintains Half-Capacity Requirement: Despite slow increases in COVID-19 cases in parts of Asia, this furniture retailer has reopened all of its stores, maintaining social-distancing mandates by operating at half capacity.

University Gears Up for Fall Activity: A technical university in southeast Asia developed strategies for conducting hybrid in-person and virtual classes, limiting on-campus dining options, and requiring masks and temperature screening.

NGO Navigates Attitudes Around Mask Use: Masks have emerged as a potential flashpoint for a nongovernmental organization (NGO) providing services for the well-being of children worldwide. The organization has to navigate which masks to provide or require in each location, and which criteria to use for resumption of activities.

Split Operations at a Food and Agriculture Firm: To limit widespread intermingling of staff, the U.S.-based firm divided employees into two groups: those who interface frequently with inter-departmental staff and those in more solitary roles.

Supplying PPE at a Clothing Retailer: A U.S.-based retailer is finding new sources of personal protective equipment to provide to employees and customers—pleasing staffers' parents, who appreciate that the corporation is prioritizing employee safety.

Dropping Physical Office Space at a Microfinance Institution: A Latin American microfinance institution will likely maintain a largely remote workforce even after an effective COVID-19 treatment or vaccination becomes available.

Travel Criteria at a Chemical Conglomerate: Business travel has resumed at a Europe-based conglomerate if employees satisfy three criteria: the journey must be business critical; neither the country of departure nor country of arrival can impose a mandatory quarantine; and the trip must be practically viable.

Manufacturer Requires Close Contact Logs: To enable contact tracing, a Europe-based polymer manufacturer requires staff to maintain a log of everyone they have come in close contact with; if people are within 1.5 meters for longer than 15 minutes, it merits an entry.

To read the latest case study updates, visit *asisonline.org/get-involved/asis-foundation/covid-19-resiliency-research/*

WEBINAR

Adapting Your Emergency Communication Plan Post-COVID-19

With changes in operational capacity and remote work, it can be challenging to know where employees are—particularly during an emergency. Organizations can leverage technology they already have to create a flexible mass notification system. Find out more in this on-demand webinar.

LEARN MORE

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

ILLUSTRATION BY *SECURITY MANAGEMENT*; PHOTOS BY ISTOCK

SEEKING CONNECTION

SECURITY AWARENESS TRAINING CAN FILL TWO ROLES: EDUCATING THE WORKFORCE AND REINFORCING COMPANY CULTURE, ESPECIALLY DURING A CRISIS. **BY CLAIRE MEYER**

COVID-19 CANCELED SECURITY WEEK. Or so John Hampson, director of global security at Kearney & Company, had thought. The weeklong program of security education and training was meant to be held in April 2020, and Hampson and his team had been developing the program for months. Then the pandemic sent the majority of employees home to work remotely.

However, security is a high priority for Kearney & Company, which contracts financial services for the U.S. federal government and prides itself on providing its clients the best-educated employees, including on security matters. In addition, the isolating effects of remote work loomed—motivating Hampson and his team to forge ahead with a virtual Security Week instead, both to maintain the organization's educational standards and foster a sense of community within the workforce, he says.

"I was seeing all this other stuff that was canceled, canceled, canceled, everything was canceled," Hampson says. "We had put a lot of effort into it; it's our paramount event of the year. People look forward to it.... It generates interest, and people love it. I saw all of these other things being canceled around the D.C. area, and so we decided to improvise."

Typically, Hampson plans a week of two to three presentations per day, with catering, outside speakers, and hands-on training to help employees engage with security in a new way. In the past, prizes, signed books, and demonstrations with security K9s have been used to garner attention, in-person attendance, and participation.

Instead, this year the security team recruited internal and external subject matter experts to record presentations in advance, and then select presenters participated in an interactive live chat at the end of the day, so employees could ask any questions or get clarification on that day's presentations. While some aspects of the in-person security awareness program could not be replicated virtually—CPR and Stop The Bleed certification, for example—other topics were adjusted to suit the current climate and virtual format. Live classes were offered around lunchtime, and employees could watch on-demand anytime.

Out of more than 700 eligible Kearney employees, more than 500 attended at least one session—approximately doubling attendance from the in-person 2019 Security Week.

In the time of COVID-19, with millions of employees working remotely, security awareness is as important as ever, says Mathew Newfield, chief information trust officer for Unisys. "Home networks are some of the most hostile networks on the planet," he says. "Most people don't know how to log into their home router, have never patched it, wouldn't know how to configure it.... If you're going to allow your employees to put those corporate assets in homes, it is worth the time as a CIO or head of IT or CISO to start doing an analysis of where your employees live, see what the main providers are and what equipment they use, and start providing some guidance on things that [employees] can do in their homes to protect themselves personally,

which will translate into protecting the organizations they work for."

Phishing and vishing attacks are on the rise, according to data from Unisys. Employees who are used to working in offices where they can quickly flag issues and get opinions from in-house experts just by walking down the hall are now isolated, and they may be less willing to send IT or security personnel an alert via email or a more official channel about a suspicious email, Newfield says.

Further compounding the challenge of security awareness mid-pandemic is employees' mental bandwidth to deal with yet another threat. According to the *2020 Unisys Threat Index,* consumers' cyber risk has taken a backseat to matters of personal and financial risk. While two-thirds of global consumers are seriously concerned about their families' health and their country's economic stability and heath infrastructure, just over 40 percent said they were seriously concerned about being scammed or experiencing a data breach while working remotely.

"In this sense, consumers appear to be taking their eye off the ball when it comes to security concerns beyond health and economic well-being, putting themselves and potentially their employers at risk," Unisys said in the report.

Newfield recommends that security leaders do their research on what employees' main concerns are, then provide guidance on personal security—such as good password hygiene, patch management, and identity theft warning signs. Especially when many corporate employees are working remotely, these personal risks also endanger business interests and assets, so this training tone can reap rewards on multiple levels, he adds.

The goal of a security awareness program is to promote the organizational and individual actions that can be taken to reduce risk and foster a culture of security, says Bryan Leadbetter, CPP. Leadbetter is a member and director of the ASIS Professional Standards Board, most recently working on the new ASIS International and (ISC)² *Security Awareness* standard, published in July 2020.

In any organization, the overall employee population will vastly outnumber the security department, he says, which means that having a robust and engaging security awareness program is key to boosting security's reach and effectiveness.

"When you look at culture within an organization, a security awareness program delivers a recognition that security is everyone's responsibility," he says. "This is a program to help people meet that responsibility and achieve a collective reduction of risk for the organization as a whole."

Conversely, the failure to have such a security awareness program, suitably tailored to the organization's needs and risk environment, could result in unnecessary loss of assets or intellectual property, business disruption, employee harm, or noncompliance with essential regulations, Leadbetter says.

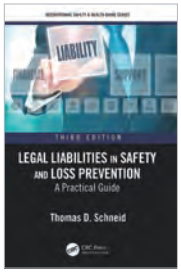
According to the ASIS *Security Awareness* standard, organizations need to consider a number of internal and external factors when developing a security awareness program, including security policies and procedures; organizational mission and core values; operating environments; security risks to the organization's employees, assets, reputation, and goals; available resources; and the roles and responsibilities of participants.

"Programs based purely on content and delivery will often fail," the

LEGAL LIABILITIES

BY THOMAS D. SCHNEID. CRC Press; crcpress.com; 390 pages; $119.95.

IN 1985, three company officials were convicted of murder in a trial regarding the death of an employee who inhaled cyanide fumes during the workday. This was a landmark workers' safety case, and it is one of many case studies examined in the third edition of *Legal Liabilities in Safety and Loss Prevention: A Practical Guide.*



This book does a superior job of explaining the purpose and history of certain acts, such as the U.S. Occupational Safety and Health (OSH) Act of 1970, which played a major role in enforcing standards and ensuring that employees are protected from hazards that could impact their well-being. Other sections address legislation, trends, safety, and loss prevention, as well as the Americans with Disabilities Act, legal liabilities under workers' compensation laws, and personal liability for safety and loss prevention professionals.

Those who have or will have responsibility for safety will gain insight into the importance safety plays in the overall well-being of organizations: good safety practices can enhance profits, and the lack of good practices may result in loss of profits and the imprisonment of those who willfully and recklessly endanger the lives of their employees.

In addition, the book does a great job providing an overall view of occupational safety and health, the importance of the OSH Act, the seriousness of compliance failure, employers' rights, and the fairness of the act in the issuance and processing of violations. A handy checklist will help practitioners prepare for safety inspections.

This third edition offers a wealth of knowledge that cannot be addressed during this brief review, but it is worth the read. Each chapter notes the key objectives contained within. For those with limited time, there is a good index to assist in locating particular topics of interest. The book focuses heavily on U.S. law, but many of its lessons could be applied in other countries.

REVIEWER: *Jim McGuffey, CPP, PCI, PSP, has been an active ASIS member since 1981, serving on several councils, as chair of the Savannah Low County Chapter, as an assistant regional vice president, and as a technical reviewer for ASIS standards. In his 26 years of holding senior positions, he has been responsible for the safety of several thousand employees.*

standard said. "Planning and careful consideration of audience and messaging are essential. Additionally, organizations should recognize that ensuring organizational relevance, establishing policies and procedures, providing ongoing communication and training, and engaging management are key factors to program success."

For example, at Kearney & Company, Hampson and his team enlisted key partners to assist in promoting the security awareness sessions in high-level meetings and with different departments. In addition, the security function sent email reminders, shared virtual posters, and leveraged internal messaging to promote the virtual program. The goal, Hampson says, was to launch a security PR campaign that was professional, polite, and not too overbearing.

Communication needs to go two ways in any successful security awareness program, Newfield says. It's the responsibility of leadership to provide guidance, and it's the responsibility of employees to ask questions, he adds. One way to encourage this interaction is to keep security education light, nonpunitive, and engaging; humorous vignette videos, lunch-and-learns, or coffee hour education sessions can be great entryways into the security conversation.

"Don't just focus on fear, uncertainty, and doubt—there's too much stress in the world already," Newfield says. This lighter, friendlier tone can also help mitigate the risk of security fatigue, triggered by an endless barrage of emerging threat information, especially when presenting security issues to nonexperts.

"These different areas are pretty complex, and we have to be able to explain how to thwart efforts at attacking our company, our people, our systems, and our laptops by these threat actors," Hampson says. "What we have to do is we have to find the right instructors."

In Hampson's case, that meant searching through recent publications and information from associations like ASIS International, asking peers for recommendations, and turning to trusted partners like the U.S. State Department's Overseas Security Advisory Council (OSAC), among others. However, security leaders should not ignore the subject matter experts within their organizations—internal security personnel can be valuable participants in security awareness programming, as much for their expertise as building personal connections between employees and their colleagues within the company's security department, particularly during times of remote work.

Several of Hampson's security team members presented during the weeklong program, and the exposure of those internal subject matter experts to the rest of the company helps employees know who to ask about security issues and builds connections for future learning.

"Even though we have all this technology, we still have to have the human angle—you have to connect with employees," Hampson says. "Even though we're using Zoom, Skype, Microsoft Teams, and all these other ways of connecting, it's not as personal as we all think it is. We need to make that extra effort."

Read about the converged security awareness program at Mastercard in this issue, page 42.

For product info #8 securitymgmt.hotims.com

GENDER EQUALITY HITS ROADBLOCKS AT WORK

A majority of U.S. adults say the country has not done enough about gender equality. Even though many believe there has been progress in the last decade, sexual harassment and societal expectations stand in the way.

ILLUSTRATION BY *SECURITY MANAGEMENT*

According to a recent Pew Research center survey, *A Century After Women Gained the Right to Vote, Majority of Americans See Work to Do on Gender Equality,* of those who think the United States still has work to do in achieving gender equality, 77 percent say sexual harassment is a major obstacle to equal rights for women. Other barriers cited are legal rights (67 percent), differing societal expectations for men and women (66 percent), and not enough women in positions of power (64 percent). Family responsibilities were cited by 43 percent of respondents as a major obstacle as well.

The vast majority of Americans surveyed (97 percent) said it is very or somewhat important for women to have equal rights with men. While 76 percent of Americans surveyed said women's societal gains have not come at men's expense, 22 percent say men have lost out in some way as society approaches gender equality.

The workplace is a key battleground when it comes to gender equality, the survey found.

When asked what gender equality would look like, 45 percent said equal pay, and an additional 19 percent said a gender-equal society would have no hiring, promotion, or educational opportunity discrimination. Among women surveyed, one in 10 said women would be more equally represented in business and political leadership. Equal respect for men and women within the workplace was cited by 5 percent of respondents.

The COVID-19 pandemic is further exacerbating existing gaps between men and women in the workplace. According to a July study from Washington University in St. Louis, the University of Melbourne, and the University of North Texas, women may face long-term employment penalties as a consequence of the pandemic. The study, conducted from February to April among 60,000 U.S. households, found that mothers of young children reduced their work hours four to five times as much as fathers, growing the gender gap in work hours by up to 50 percent. By and large, fathers' work hours had not changed.

The researchers warned that the growing gap in hours worked may result in a greater chance that upcoming promotions and raises will go to fathers and nonparents who continued working full hours during the crisis.

While mothers may be putting in fewer paid hours, they are likely working more than ever. According to the United Nations (UN), women did nearly three times as much unpaid care and domestic work as men before the pandemic, but school closures and stretched healthcare systems have increased their workloads.

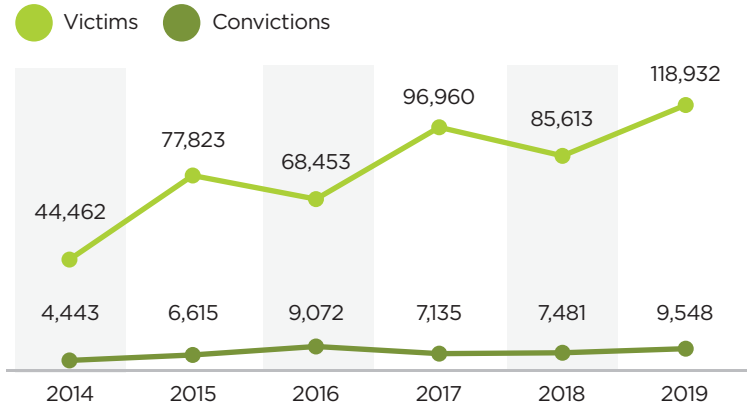
"With more than 1.5 billion students at home as of March 2020 due to the pandemic, existing gender norms have put the increased demand for unpaid childcare and domestic work on women. This constrains their ability to carry out paid work, particularly when jobs cannot be carried out remotely," the UN noted in an article, "How COVID-19 Impacts Women and Girls."

"Women's unpaid care work has long been recognized as a driver of inequality with direct links to wage inequality, lower income, and physical and mental health stressors," the article continued. "As countries rebuild economies, the crisis might offer an opportunity to recognize, reduce, and redistribute unpaid care work once and for all."

@ To read the reports mentioned in this article, visit SM Online.

HUMAN TRAFFICKING

Globally, both human trafficking victims and convictions more than doubled from 2014 to 2019; however, the increase in victims greatly outpaced the rise in convictions.



SOURCE: *Trafficking in Persons Report, 20th Edition,* U.S. Department of State, June 2020

PHOTO BY U.S. ARMY, ALAMY STOCK PHOTO

Soldiers in the U.S. Army march in the Veterans Day Parade, which honors American military veterans, in Tucson, Arizona, USA.

FRUSTRATED FORCES

NATIONAL SECURITY REQUIRES A SUSTAINABLE FIGHTING FORCE, BUT FEMALE SERVICE MEMBER RETENTION STILL LAGS DUE TO PERCEIVED BIAS AND OTHER PERSISTING ISSUES. **BY MARK TARALLO**

HOWEVER SOPHISTICATED MILITARY DRONES and artificial intelligence defense technologies have become, it still takes well-trained humans—both male and female—to sustain national security. So it follows that the national security of any nation suffers when its military has problems recruiting and retaining soldiers.

Such a problem exists for the U.S. military when it comes to female soldiers. In the 14-year period between fiscal years 2004 and 2018, women were 28 percent more likely than men to leave the U.S. military service, according to a comprehensive study recently released by the U.S. Government Accountability Office (GAO).

This low retention rate hinders the U.S. Department of Defense's (DOD) strategic plan for building the "force of the future"—defined as an all-volunteer military which draws from the broadest possible pool of talent to defend the nation for generations to come. "Recruiting and retaining female servicemembers is important in order to more accurately reflect the nation's population, ensure the strongest possible military leadership, and maintain and improve mission readiness," the GAO found in the report, *Female Active-Duty Personnel: Guidance and Plans Needed for Recruitment and Retention Efforts*.

Although women make up slightly more than half of the U.S. population, the overall percentage of female active-duty servicemembers is much lower than that, and it has stayed relatively constant—increasing slightly from 15.1 percent in FY 2004 to 16.5 percent in fiscal year 2018, according to the GAO study. The U.S. Air Force was the branch of the military with the highest percentage of female active-duty servicemembers at 20.2 percent in 2018, with the Navy at 19.6 percent, the Army at 15.1 percent, and the Marine Corps at 8.6 percent.

The GAO found that the percentage of female active-duty servicemembers began to decrease after 10 years of service, leaving a smaller pool of female personnel available for leadership opportunities. This works against the DOD's goal of increasing female military leaders.

After reviewing several studies, the GAO report found six main factors driving this increased separation rate: family planning issues, difficult work schedules, distant deployments, organizational culture factors, sexual assault concerns, and dependent caregiving responsibilities.

Another report—*Improving Gender Diversity in the U.S. Coast Guard: Identifying Barriers to Female Retention*, released in 2019 by the RAND Corporation—identifies more factors that negatively impact female servicemember retention rates.

According to the RAND report, which focuses largely on the U.S. Coast Guard, the root causes driving low retention include experiences with poor leadership, a scarcity of female role models, and a perceived gender bias that makes female servicemembers feel less valued and not respected.

For example, some of the women who participated in the RAND study's

Some women felt they often had to work twice as hard as their male peers to prove themselves to leaders who perceived them to be less capable because of their gender.

focus groups described experiences where they believed they were treated differently because of their gender or they were not offered the same career development opportunities by leadership as their male peers, Kimberly Curry Hall, a senior policy researcher at RAND and lead author of the report, tells *Security Management*.

"Some women felt they often had to work twice as hard as their male peers to prove themselves to leaders who perceived them to be less capable because of their gender," Hall says. "Other focus group participants described experiences where some leaders created work environments that were hostile to women and actively excluded them."

Other factors were concerns about sexual assault, stress related to perceived unfairness of weight standards and body fat measuring procedures, and burnout from feeling undermanned and overworked.

How can female servicemember retention be improved? A global view presents some possibilities, according to research prepared for the Defense Advisory Committee on Women in the Services (DACOWITS). The committee, which was established in 1951, provides advice and recommendations on issues related to the employment, recruitment, retention, and general well-being of the professional women of the U.S. armed forces.

DACOWITS commissioned a study in 2017 on the successful strategies that countries around the world used to attract and retain highly qualified female professionals in their respective military services. The resulting report—*Foreign Military Strategies to Recruit and Retain Women*, conducted by Insight Policy Research—discussed female retention policies for militaries of several countries, including Australia, Norway, and South Africa.

In Australia, the Australian Defense Force (ADF) has a stated goal of full gender equality in each service branch. Toward this goal, the ADF uses various measures to recruit and retain women, such as promoting the exciting lifestyle and opportunities available in the military, supporting women during the recruitment process, and minimizing the obstacles that military women sometimes encounter.

In addition, the ADF produces an annual *Women in the ADF Report* aimed at keeping the military accountable regarding recruitment and retention goals and gender-related issues.

HOMELAND SECURITY

BY EHSAN ZAFFAR. Routledge; Routledge.com; 568 pages; $39.95.

AUTHOR EHSAN ZAFFAR presents a broad-based and intelligent overview of homeland security in the United States throughout his book *Understanding Homeland Security: Foundations of Security Policy.* The book is well-organized, well-written, and easy to follow.

The publication covers historical factors of homeland security (both before and after the seminal events of 9/11), complicated concepts pertaining to immigration, the protection of the U.S. borders (including assessing and mitigating risks), and topics pertaining to intelligence gathering, cybersecurity, legal concepts, civil rights and civil liberties, and protection methodology for organizational sectors including transportation and critical infrastructures. In addition to this content, the author also presents impressive "added content" through question-and-answer sections from a wide range of experts, including law enforcement and security industry professionals, academics, and two former U.S. secretaries of homeland security (Tom Ridge and Janet Napolitano). The scope of general knowledge of the book is impressive.

Although the book includes excellent information from governmental and law enforcement sources, it lacks a global view of protection and terrorism. The reader needs to understand that the book revolves around the American protection of the homeland and is not a worldwide review or report of such issues. Equally important is that the book offers the reader little information regarding how the private security sector contributes to the defense of the homeland. If the reader is seeking a global or security industry content, this book will not satisfy their needs.

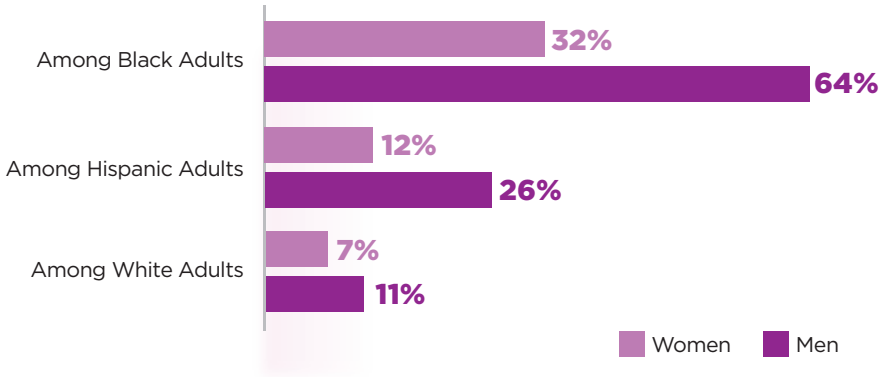
Intended as a college-level textbook, the volume makes an adequate primer that highlights key terms, poses thought-provoking questions, and delivers intriguing and informational pictures and figures in each chapter. It would be appropriate for mid-level undergraduate (200 and 300 level) students. The publisher offers the book in hardcover, softcover, and electronic formats. Also important is that publisher promotes instructor resources, assisting in course preparation. The security professional may not find much useful or specific information other than a wide review of topics and general information pertaining to the governmental management of infrastructure in protecting the American homeland.

In summary, *Understanding Homeland Security: Foundations of Security Policy* is a useful exploration of American homeland security protection and appropriate supportive concepts intended for undergraduate academic use.

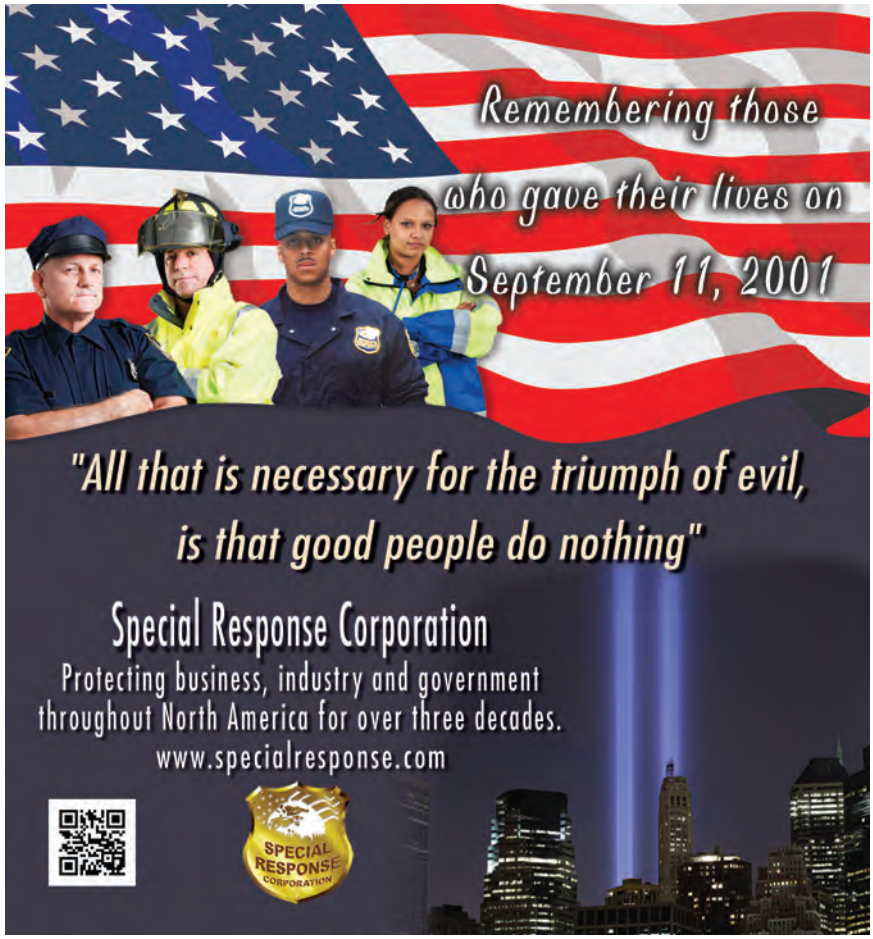
REVIEWER: *Joseph Jaksa, CPP, is a professor of criminal justice at Michigan's Saginaw Valley State University and is a member of ASIS International.*

ON BEING STOPPED BY POLICE

Nearly two-thirds of American Black men say they have been unfairly stopped by police because of their race or ethnicity; in comparison, about one in four Hispanic men and one in 10 white adults say they have been unfairly stopped by police.



SOURCE: *Amid Protests, Majorities Across Racial and Ethnic Groups Express Support for the Black Lives Matter Movement,* Pew Research Center, June 2020



For product info #9 securitymgmt.hotims.com

In Norway, the military used unique female retention strategies such as unisex lodging and all-women training programs. Moreover, women have achieved the highest levels of Norwegian military leadership; since 1999, five women have served as Norway's Minister of Defense. This has been an effective role modeling tool, the report found. The importance of role modeling also came up in the RAND study—the desire to be a role model to other women encouraged some focus group participants to continue their Coast Guard careers, Hall says.

In South Africa, the National Defense Force (SANDF) offers maternity leave with full pay for a period of up to four months. During this time, a woman on leave can still be considered for normal promotions. "Maternity leave policies are an important contributor to women's retention in any workplace," the DACOWITS report says.

In the end, Hall says that efforts to ensure women are represented at all levels can strengthen military services because organizations with a wide

Since 1999, five women have served as Norway's Minister of Defense. This has been an effective role modeling tool.

range of viewpoints in a positive work culture can foster creative ideas that improve operations.

"Individuals with different demographic background characteristics, such as different genders, can bring diverse perspectives to the workplace," Hall says. "When these differences are harnessed effectively in an inclusive environment, it can drive innovation."

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

GEARED FOR POWER + PERFORMANCE

ALTRONIX MIDSPANS AND SWITCHES ARE DESIGNED WITH MAXIMUM FLEXIBILITY FOR DEPLOYING IP DEVICES. NETWAY PROVIDES THE PRECISE COMBINATION OF SPEED AND SCALABLE POWER IN VIRTUALLY ANY ENVIRONMENT.

WHAT'S DRIVING YOUR PoE?

Altronix

Netway®

Now Offering 802.3bt 4PPoE Solutions!

MADE IN THE U.S.A. ALTRONIX.COM LIFETIME WARRANTY

For product info #10 securitymgmt.hotims.com

PHOTO BY ISTOCK AND *SECURITY MANAGEMENT*

DISTRICT UPGRADES

AS PART OF A CONTINUOUS SECURITY IMPROVEMENT PROJECT, A LONG ISLAND SCHOOL DISTRICT ADOPTS A NEW SYSTEM TO UPGRADE ITS LOCKDOWN CAPABILITIES. **BY MEGAN GATES**

LOCATED IN LONG ISLAND, New York, Jericho Union Free School District is known for its academic prowess and a history of fostering students to achieve national recognition. In spring 2020, while students and staff worked from home to slow the spread of the coronavirus, a team of students from Jericho High School won first place in the Lexus Eco Challenge.

The team, dubbed Finding Nano, created its own sustainable ultrafiltration membrane system—and an app—to help residents monitor water quality after they discovered that 61 percent of New York waterways are contaminated with unregulated, potentially carcinogenic contaminants.

"They reached out to water authorities and demonstrated how current wastewater-treatment processes are inadequate and encouraged using nanocellulose-based filtration systems," according to the competition's website. "Finding Nano then formed an international network of Finding Nano Ambassadors to encourage high school environmentalists to express their local concerns, learn sustainable practices from each other, and educate their communities. They also collaborated with UN delegates to maximize sustainable efforts."

And while the district's 3,200 students and 1,000 employees spent the last part of the 2020 spring semester learning and teaching from home, Director of Facilities Mike Hahn was hard at work to ensure that when students and staff do return to campus, they can safely continue their pursuit of excellence.

Hahn started working at the district eight years ago, and he is responsible for capital improvements, maintenance, and security at one middle school and high school facility, three elementary schools, and one leased facility. When he took over his role, the district had no real security system or procedures in place. Since then, Hahn has introduced an access control system, ID tags for employees, security vestibules, and a visitor check-in process.

Once the perimeter security was enhanced, however, Hahn knew that the next step was to create the ability to initiate a lockdown within the district's facilities to respond to an emergency situation, such as an active shooter.

In 2018, the district began looking at various products at security showcases. Hahn says school officials were specifically looking for a system that would work with the district's existing master key system.

"We did not want to have to rekey the entire district, or recore the locks in the district," Hahn explains. "We were looking for something that could accommodate taking the core out of the existing locks and putting it in the new product, and that could operate with my ID cards."

Adopting such a solution would allow the district to phase out issuing keys for the doors and create a system where teacher and staff ID cards were programmed to provide access to the doors they needed to be able to open at their specific facility.

The district also wanted a lock solution that had a lever handle so the doors would be compliant with the Americans with Disabilities Act.

After a review of products, the district chose Dormakaba's E-Plex 7900 wireless locks with Aurora Advanced Lockdown software licenses.

The software system allows the district to program teacher and staff ID cards to provide access based on their needs—for instance an elementary school teacher could use her ID card to open doors only in her building instead of the entire district.

"We program teachers' cards, so they start at 6:30 a.m. and shut off at night at 6:00 p.m.—there's no access to the building whenever you want it," Hahn adds.

After the lock was selected in early 2018, Hahn led a districtwide project to remove the existing door locks from approximately 800 doors, take out the cores, and install the new Dormakaba lock cores.

"We figured if we're going to do it, we're doing it districtwide," Hahn says. "We can't present this to the public as a security issue and then decide we're only going to do one school. We can't tell the public the kids in this school are more important than somewhere else."

The introduction of the security procedures and the Dormakaba system required a culture change in the district, Hahn says.

"Parents used to come into the building as they wanted," he says. "When you're used to doing that, it's a bit of a culture shock, but most people—with all of the shootings that have happened—realized how lax things were and that something needed to be done."

The project was initially supposed to be finalized before the beginning of the fall 2018 semester, but there were some snafus in the process.

While removing the cores from the old locks, the installation team did not label which core went to which door. This resulted in a very time-consuming process to match the cores to the appropriate door and new lock, Hahn says.

Once the locks were installed, the district also worked with its integrator—Intralogic—to address some programming challenges related to the software and antennas the locks rely on.

There was an initial miscalculation, Hahn says, about how many antennas would be needed for each facility in the district to allow the locks to communicate wirelessly.

"The locks were sending out signals—almost like roaming," Hahn says, adding that this caused the locks' batteries to die sooner than anticipated. The district has since added additional antennas and the integrator replaced the batteries.

One programming challenge the district had to work through was related to the specialized lockdown software—Aurora Advanced Lockdown—it purchased to run on the system. Using strategically placed panic buttons throughout facilities, the software allows an individual who pushes that button to issue a prerecorded message announcing a lockdown over the loudspeaker system while also locking all the doors in the building. This method was preferable to the previous one, which Hahn says required a principal to login and initiate a lockdown.

"It's a much better situation to have a panic button so trustworthy people—administrators, staff members—can feel empowered to initiate it," Hahn says.

The software functioned perfectly to initiate a lockdown, but there were some bugs that prevented the district from lifting the lockdown after an all-clear message was issued. Intralogic came in and was able to address the issue, Hahn says, so now the lockdown can be lifted.

The original installation was for approximately 800 doors, but it did not include the bathrooms at any of the buildings. These have traditionally always been unlocked, but with the rise of school shootings, Hahn says the district decided these rooms should also be lockable to allow students and staff to shelter in place should an incident occur.

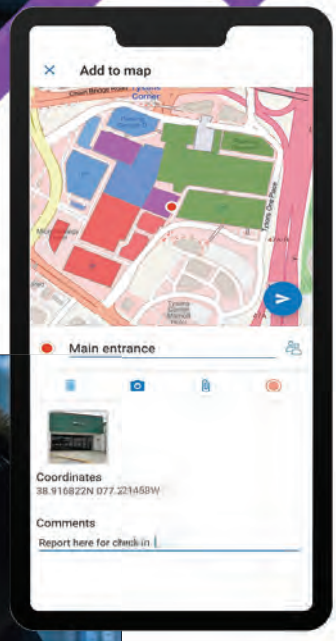
The district planned to install this new wave of locks during the summer of 2020 with the help of funding from the New York Governor's Office. But with the coronavirus pandemic, those plans have been put on hold.

"Right now, there's a lack of state aid that the governor was talking about sending back to the schools—we can no longer count on that coming from the state, and our priorities have shifted to looking at what we need in place to safely reopen," Hahn says. Funding may instead go towards sneeze guards and other personal protective equipment that schools may be required to provide upon reopening.

Additionally, Hahn says there are plans to work with Intralogic and Dormakaba to offer a training session on locksmithing with district facilities staff, to allow them to address common maintenance issues in-house. That will have to wait, however, until the pandemic subsides and it's safe for the training to be conducted in person.

For more information: *www.dormakaba.com*; 1.800.849.8324

Mission managers can monitor team member locations, tracks, connectivity, chats, and images from the field, all in one place.



The ArcGIS Mission mobile app for iOS and Android allows field operators to view and share data about their team members on their mobile devices.

Improve Situational Awareness and Mission Management with ArcGIS® Mission

ArcGIS® Mission is a command and control system that organizations—from disaster response and law enforcement agencies to executive protection and event security teams—can use to streamline mission management, gain situational awareness during active missions, provide geospatial-based peer-to-peer communication in the field, and conduct postmission reviews. The software enables teams to better understand their operations, make informed decisions in real time, and acquire new understanding from completed missions.

Some key features include the following:

- **One platform:** Use one platform to effectively plan, manage, execute, and review mission operations.
- **Tactical situational awareness:** Know where mission members are and coordinate actions among team members based on real-time events and activity.
- **Peer-to-peer communications:** Persistent peer-to-peer (P2P) communication enables teams to share location, tracks, and messages for stronger collaboration in disconnected environments.
- **Improved understanding:** Establish a common understanding of post-event-related activities and identify lessons learned to drive organizational change.

ArcGIS Mission Manager enables mission leaders to quickly create, define, assign team members to, and manage missions in their ArcGIS organizational account.

The three components of ArcGIS Mission are as follows:

- **ArcGIS Mission Manager** is a premium app that organizations can use to manage their missions, assign mission members, and distribute mission content.
- **ArcGIS Mission Responder** is a mobile app that mission members can use in the field to share location tracks, map markups, and photos.
- **ArcGIS Mission Server** is software that enables peer-to-peer communication among all mission team members.

What's Your Mission?

To learn more, contact an Esri representative at **go.esri.com/arcgis-mission**.

esri® THE SCIENCE OF WHERE®

Copyright © 2020 Esri. All rights reserved. Esri, the Esri globe logo, The Science of Where, ArcGIS, and esri.com are trademarks, service marks, or registered marks of Esri in the United States, the European Community, or certain other jurisdictions. Other companies and products or services mentioned herein may be trademarks, service marks, or registered marks of their respective mark owners.

G1187006

ILLUSTRATION BY MICHAEL AUSTIN

BOLSTERING TRUST

ORGANIZATIONS ARE INCREASINGLY MAKING THEIR SECURITY AND PRIVACY POLICIES A CORE COMPONENT OF THEIR BUSINESS. THE MOVE COULD ALSO BOLSTER CONSUMER TRUST IN THEIR BRANDS.

BY MEGAN GATES

WHEN THE WORLD MOVED indoors and online in early 2020 as the coronavirus spread, one common theme emerged: everyone seemed to be hanging out on Zoom.

Zoom meetings, long a staple for many organizations using the enterprise version of the video conferencing product, became the venue for virtual education, happy hours, birthday parties, game nights, family dinners, and first dates.

Usage of the product "ballooned overnight," from approximately 10 million daily participants in December 2019 to more than 200 million daily meeting participants in March 2020, according to Zoom.

But with that rise in usage also came skepticism that Zoom's platform was as secure as the company had originally claimed. Initially, the company suggested that Zoom meetings were end-to-end encrypted, but privacy advocates and researchers later said that was inaccurate and criticized Zoom for providing users with a false sense of security.

"As long as you make sure everyone in a Zoom meeting connects using 'computer audio' instead of calling in on a phone, the meeting is secured with end-to-end encryption, at least according to Zoom's website, its security white paper, and the user interface within the app," according to The Intercept. "But despite this misleading marketing, the service actually does not support end-to-end encryption for video and audio content, at least as the term is commonly understood."

Instead, Zoom was offering transport encryption—the same type of encryption used for HTTPS websites, meaning some Zoom meeting data was not private from Zoom itself.

After The Intercept's story broke on 31 March, criticism poured in across the Internet from teachers who were discouraged from working with the product to U.S. federal government agencies that halted use of the product.

In response, Zoom—which did not return a request for comment on this article—issued a blog post acknowledging that it had "fallen short of the community's—and our own—privacy and security expectations" and was taking steps to address them.

"These new, mostly consumer use cases have helped us uncover unforeseen issues with our platform," Zoom CEO Eric S. Yuan wrote. "Dedicated journalists and security researchers have also helped to identify pre-existing ones. We appreciate the scrutiny and questions we have been getting—about how the service works, about our infrastructure and capacity, and about our privacy and security policies. These are the questions that will make Zoom better, both as a company and for all its users."

The next steps Yuan outlined included offering additional training and tutorials for users, addressing problems to reduce Zoombombing (when uninvited parties break into and disrupt sessions), conducting a review of third-party experts and representative users, preparing a transparency report, launching a CISO council, enhancing its bug bounty program, and conducting white box penetration tests.

In June, Zoom announced that it would make end-to-end encryption an advanced add-on feature for all its users—not just paid subscribers as previously planned.

"Zoom's decision to offer end-to-end encryption more widely is especially important because the people who cannot afford enterprise subscriptions are often the ones who need strong security and privacy protections the most," said the Electronic Frontier Foundation (EFF) in a blog post on the decision. "For example, many activists rely on Zoom as an organizing tool, including the Black-led movement against police violence."

The decisions made by Zoom reflect a broader trend when it comes to the relationship institutions have with the public: the need to balance competence with ethical behavior. The finding comes from the *2020 Edelman Trust Barometer* report, published in January 2020 as the latest installment in the firm's annual evaluation of consumer trust.

The report found that less than half of the overall surveyed population trusted institutions to do what was right, and that most people said institutions only served the interests of the few—not everyone equally or fairly.

"The informed public—wealthier, more educated, and frequent consumers of news—remain far more trusting of every institution than the mass population," according to the report. "In a majority of markets, less than half of the mass population trust their institutions to do what is right."

Edelman also found that a growing percentage of customers are "belief-driven buyers," or those who believe brands are agents for change—and by spending money with that brand, the individual is making a decision to approve what that brand stands for.

"Trust is undeniably linked to doing what is right," according to Edelman. "After tracking 40 global companies over the past year through our Edelman Trust Management framework, we've learned that ethical drivers such as integrity, dependability, and purpose drive 76 percent of the trust capital of business, while competence accounts for only 24 percent."

When it comes to cybersecurity and protecting consumer's data, there is a "tenuous balance between trust, security, and privacy," says Linda Walsh, managing director at Deloitte & Touche LLP and cyber risk services data solution leader for Deloitte Risk & Financial Advisory.

"At a granular level, we're seeing more businesses try to understand that intersection between privacy and identity," Walsh explains. "What I mean by that is we've had that regulatory landscape around [the California Consumer Privacy Act] and [the General Data Protection Regulation] that has a lot of rules and regulations around data. Some companies were a little on their heels for that, and they looked at it as just a regulation. Other companies have embraced it and understand that privacy and trust issues can be a brand differentiator."

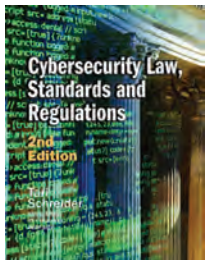
Some of the most prominent examples of this are technology companies, which Walsh notes have been successful at saying privacy is a pillar component of their business and explaining why they can be trusted by consumers.

"I think what we're going to see as time goes on is people understanding that privacy and trust go hand in hand," she adds.

CYBERSECURITY LAW

BY TARI SCHREIDER. Rothstein Publishers; Rothstein.com; 324 pages; $89.95.

INFORMATION security generalists who wish to look up relevant laws and court decisions on legal issues will find a highly useful resource in the second edition of *Cybersecurity Law, Standards and Regulations.* Readable and well-organized, the text is especially valuable for quick searches. Text boxes throughout the book highlight key ideas. Each chapter has self-study questions, making the book suitable for use as a textbook. (This reviewer teaches cyberlaw and will use the text as a standby reference.)



While the work has an extensive index, it does not offer a centralized glossary. Legal texts present many new terms and concepts, so providing a glossary could help the reader refresh definitions with relative ease. On the other hand, the book's appendix is a great strength. Its "helps" range over seven topics, including eDiscovery software, cybercrime reporting agencies, cyber tort readiness checklist (useful in civil litigation), providers of cyber liability insurance, digital forensics toolkits, cyber liability stress test, and information about establishing a cybersecurity law program. In addition, a list of references serves as an effective research resource. The text, generous in summarizing facts and ideas, also includes numerous tables, which increase understanding.

Relevant cybersecurity legal concepts are discussed broadly. Topics covered in the main discussion include cybercrime taxonomy, basic elements of law (criminal law and torts), extradition (international), U.S. cybersecurity law, privacy and data protection, cryptography and digital forensics law, and future developments in the field.

Other key topics that receive deserved coverage include common causes of cyber legal case dismissal, "Fifth Amendment and Data Encryption," the right to avoid self-incrimination and cryptographic decryption, and what courts can do to compel evidence about cryptographic keys and passwords. In addition, the European Union Cybersecurity Act discussion provides helpful information for the professional working in the European arena.

While this book is not a substitute for actual legal counsel, the text does supply a yardstick for the information security generalist trying to get an initial handle on a cybersecurity legal issue.

REVIEWER: *Ronald L. Mendell, CISSP, is a member of ASIS and a faculty member of the College of Information Technology at Western Governors University, where he teaches information security. He is also a consultant who writes about physical and information security.*

This shift is due—in part—to increased awareness among consumers about how their unique data is often the most valuable asset organizations have. Consumers are increasingly looking for more control over their data, and for organizations to be transparent with them about the data they are collecting and using.

Organizations are also realizing that trust must be earned—it cannot be taken as a given—and they need to continuously treat protecting consumers' privacy as an active component of the overall business.

"You're an active participant, not a passive participant," Walsh adds. "This means demonstrating that you're managing their data—where it goes, how it's used, and that consumer requests for data are fulfilled—that builds a basis of trust."

Roey Eliyahu, CEO and cofounder of Salt Security, a firm that specializes in protecting assets from application programming interface (API) attacks, agrees and adds that organizations must be transparent about the security policies and procedures they have in place to protect customer data.

"To create a great trusted brand from a security and privacy perspective, you have to be transparent," he says. "If you're not and there's an issue, consumers will not trust you to fix it."

One business that's done a good job of this, Eliyahu says, is Apple, which has been vocal over the past few years about steps it's taking to ensure customer data remains private—even from the U.S. government.

In 2016, the FBI initiated a legal battle against Apple to require the manufacturer to unlock the iPhone that belonged to the gunman responsible for the San Bernardino, California, shootings that left 14 people dead.

Apple refused to create a method to provide the FBI access to the iPhone; CEO Tim Cook issued a statement at the time that said the "implications of the government's demands are chilling."

"The government would have us remove security features and add new capabilities to the operating system, allowing a passcode to be input electronically," Cook said. "This would make it easier to unlock an iPhone by 'brute force,' trying thousands or millions of combinations with the speed of a modern computer."

The decision was widely viewed as a win for Apple, and it increased trust in the brand and its security and privacy policies. Consumers and customers are increasingly making similar demands from other businesses, Eliyahu says.

For instance, Salt Security has put together a complete security overview document that details all aspects of the firm's security—who has physical access to its facilities, how customer data is stored, and the measures taken to protect that data.

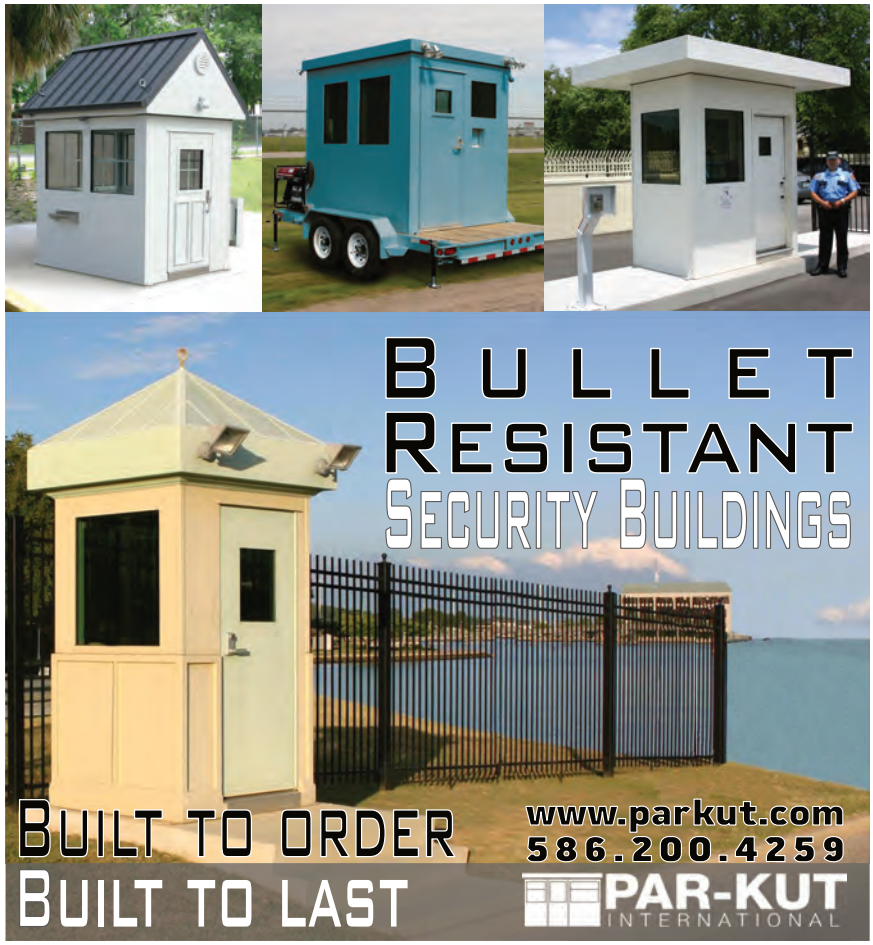
"When you have it all organized, that's how they know you're being strategic about your own security," Eliyahu says.

That posture reflects Edelman's findings about what institutions—especially businesses—can do to foster trust with customers. For instance, 73 percent of those surveyed said companies can take actions that both increase profits and improve conditions in the communities where they operate.

CEOs and executives can also speak out on the major issues of the day—such as automation, the ethical use of technology, diversity, and climate change—to show how their organizations are leading change, instead of waiting for regulators to impose it, according to Edelman.

"Business must take the lead on solving the trust paradox because it has the greatest freedom to act," Edelman explained.

@ To read the Edelman report, visit SM Online.



For product info #13 securitymgmt.hotims.com

THE CHALLENGES OF YESTERDAY ARE NOT THE CHALLENGES OF TOMORROW

Allied Universal® is There for you™, keeping you secure by staying one step ahead of tomorrow's growing and evolving threats.

Because it is when we are fearless, humanity thrives.

aus.com

©2020 Allied Universal

ALLIED UNIVERSAL®
There for you.

For product info #14 securitymgmt.hotims.com

SEEDS OF DISRUPTION

The world is entering a decade of rage, unrest, and shifting geopolitical sands. Security leaders need to understand the factors behind mass protests to accurately predict them and mitigate their effects.

"We are living in an age of mass protest," the Center for Strategic and International Studies (CSIS) said in a March report looking back at 2019.

With at least 37 countries experiencing mass protests, these movements globally surged in 25 percent of countries throughout 2019, intensifying toward the year's end in Hong Kong, Chile, Nigeria, Sudan, Haiti, and Lebanon. Virtual uprisings joined physical unrest, and Internet shutdowns were increasingly common, with India, Pakistan, Syria, and Turkey leading the world in this regard.

Historically unprecedented levels of unrest continued to increase in early 2020, then simmered in the background during the first months of the COVID-19 pandemic and related lockdowns. Mass protests in the United States surged by 186 percent from April to May, largely catalyzed by the killing of George Floyd in Minneapolis, Minnesota. By June, the country fell into the high-risk category of Verisk Maplecroft's *Civil Unrest Index*, an assessment of the risk of disruption to businesses due to mobilized social disruptions as a reaction to economic, social, or political issues. Similar spikes occurred in the United Kingdom, Germany, Spain, Sweden, and France, while mass protests continued in Hong Kong and Lebanon.

PHOTO ILLUSTRATION BY *SECURITY MANAGEMENT*; PHOTOS BY ISTOCK

The economic fallout of mass protests and their potential impact on corporate operations cannot be overstated, as civil unrest triggered losses of billions of dollars for businesses, national economies, and investments worldwide. Though recent mass protests appeared to start quickly, multiple long-unaddressed issues provided protesters with a fuel reserve of frustration.

THE BACKDROP

"Mass protest" is a complex term, taking on different meanings depending on the environment. It does not equal violent protest; however, the potential for morphing quickly into violence is real. Understanding how a mass protest may manifest in a certain environment will greatly improve resilience planning.

The media attention to mass protests around the world implies they come on suddenly, without warning. Yet, as illustrated in CSIS's *The Age of Mass Protests: Understanding an Escalating Global Trend,* civil unrest and mass protests are the result of years' worth of issues affecting large population centers in each region of the world. The 2020 surge in protests is not surprising given that, over the previous decade, anti-government protests increased by nearly one-third in 114 countries. From at least as far back as the Arab Spring, the issues that underpin many recent uprisings—including the Black Lives Matter (BLM) movement, anti-government movements, and economic outrage—remain unaddressed and are compounded by present frustrations, including COVID-19 conspiracy theories and anti-lockdown sentiments.

Both developing and advanced economies have had their share of reasons that stoked unrest. Civilian anti-government protests grew at a faster rate in Europe and North America than the global average. Between 20 January 2017 and 1 January 2020, nearly 11.5 million Americans participated in 16,000 protests across the country, including the five largest demonstrations in U.S. history, according to the CSIS. Thousands protested across France as part of the Yellow Vest movement. During one of France's most important holiday periods, more than 800,000 people participated in weeks of mass demonstrations in Paris.

From 2019 to 2020, the number of countries rated as an extreme risk—making them some of the riskiest locations in the world—in the *Civil Unrest Index* jumped up by 66.7 percent. These latest additions include Ethiopia, India, Lebanon, Nigeria, Pakistan, and Zimbabwe. Meanwhile, Sudan has overtaken Yemen as the country with the highest risk globally.

Though mass demonstrations in 2020 were initially dampened by the COVID-19 pandemic, this is unlikely to change the overall trend. Mob violence has increased since the World Health Organization (WHO) categorized the novel coronavirus as a pandemic in March 2020, according to the Armed Conflict Location & Event Data Project (ACLED). Approximately 1,100 protest events were recorded in about 90 countries. Bulgaria, Greece, and Germany saw protests fueled by unfounded conspiracy theories blaming various targets—including 5G networks, George Soros, and Bill Gates—for the pandemic.

Mass protests will very likely continue, if not increase, over the next few years if the root causes remain unaddressed. In fact, the CSIS predicts that the 2020s will become the "decade of rage, unrest, and shifting geopolitical sands."

Over the previous decade, anti-government protests increased by nearly one-third in 114 countries.

DRIVERS OF CIVIL UNREST

The rage that boiled over into street protests this past year caught many governments by surprise. Authorities generally reacted to such disruptions with limited concessions and a clampdown by security forces, leaving the underlying causes unaddressed. Even if governments committed to managing the issues frustrating protesters, solutions to the complex challenges that precipitated the unrest are not quickly or easily available.

Globally, companies and investors will have to adapt to mass protests as a "new normal" for the foreseeable future, according to *Political Risk Outlook 2020*. Although corporations often turn to CSOs to explain mass protests—usually after the fact—security leaders can better serve their organizations by improving forecasting of a mass disruption and its impact based on its cultural context.

There is no crystal ball foretelling when and how a mass protest may begin. Looking more broadly at geopolitical, regional, and internal issues—and the connections between them—helps build the picture over time. No single source of information will predict a mass protest. There are, however, various economic and societal indicators that can provide foresight into how the situation will likely evolve.

Economic hardship and significant fluctuations are often the most important drivers of a mass protest. Unaddressed economic stressors eventually result in hardship and discontent throughout a population.

Overall, economic stress arises from shifts in the pattern of economic behavior. Growth may continue, but a dramatic slowdown can have significant consequences, affecting social structures and political stability.

A forecast by Geopolitical Futures predicted a global economic slowdown for 2020, partly due to a cyclical downturn. Normally this would not trigger major social, political, and international crises; however, other factors

PHOTO BY ROBERTO AROSIO, ALAMY STOCK PHOTO

Thousands of demonstrators in Madrid, Spain, protested for social justice on 7 June 2020.

will exacerbate the impact of this slowdown, generating substantially more non-economic consequences than normally anticipated.

For example, some nations did not successfully adapt to the changes necessitated by the 2008 global financial crisis, and the economic disparities experienced by citizens in those countries remain unaddressed.

International issues further stressed populations and systems, specifically food shortages aggravated by a horde of migrating locusts and the COVID-19 pandemic—the latter triggering forced and prolonged shutdowns of businesses worldwide. The shuttering of economies globally resulted in the worst economic downturn in 300 years, according to the Bank of England. George Freeman, founder of Geopolitical Futures, estimated that the unemployment rate is expected to reach 20 percent in the United States, with the greatest impacts hitting the disadvantaged.

Economic stress indicators alone will not paint a full picture, though, for those looking at how an area's residents may behave or react in the future. Understanding a region's culture, characteristics, and unique societal structure can help form a better gauge and a more informed response to potential mass reactions.

When looking at CSIS data analysis related to mass protests since 2009, these events have increased around the world by 15 percent. A broad view shows that events such as the Arab Spring were not isolated phenomena, but rather acute manifestations of global trends. One root cause of discontent was the rollback of civil and human rights, which began as far back as 1997, according to CSIS's *The Age of Mass Protests*.

Environments with poor human rights records—such as high rates of extrajudicial killings, arbitrary arrests or detentions, and torture—should be monitored to determine their long-term ability to offer businesses a viable market. The research firm Verisk Maplecroft's *Security Forces and Human Rights Index* rates 36 countries as extreme risk, including emerging markets where corporations or investors may be seeking to do business.

Human rights violations, including arbitrary arrests and the use of indiscriminate violence against peaceful mass protests, pose a risk to both demonstrators and any company staff in the vicinity of ongoing unrest. The use of violence eventually radicalizes protesters, provokes violent responses, and ultimately fuels further unrest, according to *The Political Risk Outlook 2020*.

Systemic corruption levels also contribute to expressions of societal frustrations and mass protest. Transparency International monitors corruption levels globally and advocates for change. On Transparency International's 100-point scale, where 100 is the "cleanest," two-thirds of countries measured fell below 50, and the average of all nations was only 43.

In its *CPI 2019 Global Highlights* analysis, Transparency International further argues that the influence of large money in political campaigns in developed democracies fuels the increasing division between opposition groups, often resulting in mass protests.

POTENTIAL FALLOUT

Along with broader economic and infrastructure costs, a mass protest prevents business operations in and around the area of protest. It hinders and blocks the ability for personnel, supplies, products, and customers to travel to, from, or through impacted areas. In the short

term, mass protests reduce tourism, which many smaller businesses rely on.

As detailed in Verisk Maplecroft's *Political Risk Outlook 2020*, a seemingly minor issue of a 30 peso ($0.04 USD) increase in metro fares in Chile triggered mass protests in October 2019. The first month of demonstrations cost the economy and infrastructure billions of dollars—not solely from the interruption of regular economic activity and destruction of resources, but also because of revenue sources that avoided the country. The 2019 United Nations Climate Change Conference was moved from Chile to Spain, and the Asia-Pacific Economic Cooperation forum was canceled.

In extreme instances, mass protests directed at corporate facilities can result in injury to personnel, significant repair costs, and loss of productivity. Blocking off operations in one country can have downstream effects on supply chain movement. Additionally, from a trade or supply chain perspective, mass protests create uncertainty capable of leading corporations and investors to postpone plans while awaiting outcomes. As seen in the Chilean protests, this can inhibit inbound foreign investment; if potential investors are nervous about a country's political stability, they will postpone critical investment decisions—which could have a devastating impact on global markets. Mass protests can also result in corporations' deciding to relocate their facilities or, even worse, forcing them to go out of business.

This impact is amplified when investors and corporations inside a country seek to move assets to safer locations, according to William Reinsch, a senior adviser and Scholl Chair in international business at CSIS and co-host of *The Trade Guys* podcast. This double hit to the local economy often results in greater instability and increased unemployment, boosting the existing frustrations that likely catalyzed the initial unrest.

Solutions to the complex challenges that precipitated the unrest are not quickly or easily available.

Although the C-suite often looks to its CSO to mitigate mass protests with measures like forecasting and planning appropriate responses to disruptions, few corporations support methods that enable resilience. The majority of CSOs are highly competent in ensuring facilities' physical security, yet when it comes to mass protests, there are additional factors that account for successfully mitigating risk.

It is critical that CSOs and the C-suite understand cultural impacts and how mass protests manifest in individual environments. A $0.25 per gallon gasoline price hike in the United States may be aggravating but will go unnoticed by most. However, a reduction in fuel subsidies and a resulting $0.10 per liter price increase in another country can bring tens of thousands to protest in anger in the street.

Broad-based situational awareness leverages political instability and mass demonstration forecasting to successfully prepare an organization and develop an appropriate response. Improving a corporation's understanding of the geopolitical and local context enables operational preparedness rather than allowing for operational interruptions in response to mass protests. There are numerous corporate subscription services that provide forecasting information, ranging from smaller options to enterprise subscriptions with direct access to analysts, as well as nonprofit analyses available at no cost.

Although analysis and forecasting can better connect and prepare an organization, this does not imply that the responsibility of a successful response falls entirely on the shoulders of the CSO. An integrated and collaborative C-suite can bring additional resources to bear, appropriately sharing information within an organization. Collaborative discussions across investment, operations, finance, security, and executive departments help better divide subject matter into more manageable components. Establishing these tools and improving collaboration enable the CSO to better advise the organization.

METHODS AND MOBILIZATION

Though mass protests are nothing new, recent years show an evolution of sympathetic groups connecting across the globe through the use of the Internet. Sympathizers share tactics and information, sometimes creating additional protests in other countries to show support on a given issue.

In 2008, during the height of the global financial crisis and prior to the Arab Spring, former U.S. National Security Adviser Zbigniew Brzezinski identified a "global political awakening." Brzezinski argued that a new era of global activism had dawned.

"For the first time in history, almost all of humanity is politically activated, politically conscious, and politically interactive," he wrote.

The BLM, white nationalism, and environmental protests across multiple continents in 2020 illustrate Brzezinski's point. Activism is on the rise, and the Internet has connected groups across borders.

Whether blocking city centers or targeting infrastructure, modern mass protestors have learned new tactics, as well as logistics to counter security force moves. In Hong Kong in 2019, activists developed an entire supply line to ensure the availability of materials to demonstrators. These supplies included umbrellas to use as shields, laser pointers to blind cameras, scissors, and Allen wrenches used to dismantle police barricades. Protesters even repurposed police barricades to create their own defensive lines. These tactics were shared over social media with other protest movements.

Throughout multiple areas in Spain during 2018, millions of residents protested peacefully in support of different causes. Although they were nonviolent, hundreds of thousands of supporters of Catalonia separatism protested in Barcelona over multiple days, tying up the city center. During the same period in Madrid, approximately 1 million protestors staged a peaceful counter-protest to Catalonia separatism.

Learning from the Hong Kong protest groups, Catalonians changed their peaceful tactics in 2019 and forcibly occupied an airport, disrupting flights. Protestors also blocked major highways, significantly delaying the movement of goods around the area.

This evolution prepares protest groups to withstand security force interventions for longer periods, prolonging the impact on a region's businesses.

For the first time in history, almost all of humanity is politically activated, politically conscious, and politically interactive.

In more extreme cases, mass protests can turn violent, directly targeting businesses and government infrastructure. Vietnam is a country with very few protests, and those that do occur are typically small and peaceful. However, in 2014, what started out as mass protests against a Chinese oil rig in the South China Sea quickly turned into anti-Chinese business riots, resulting in millions of dollars in damage and 29 deaths.

Throughout much of the second quarter of 2020, mass protests and violent riots occurred in multiple U.S. cities, sparked by the killing of George Floyd. Long-unaddressed systemic racism issues in the United States provided a fuel reserve for the protests. U.S. National Guard units were called in to several areas to support local police as businesses, police stations, and cars were looted and burned, in addition to the killing of police and civilians during the riots. Police used tear gas and rubber bullets, resulting in serious injuries.

Though the bulk of these mass protests centered around the BLM theme, the violence in these instances resulted from a growing patchwork of participants piggybacking onto the mass protests. In a May 2020

For product info #16 securitymgmt.hotims.com

New York Times article, Brian Levin, director of the Center for the Study of Hate and Extremism at California State University and a former New York City police officer, said: "We're going to see a diversity of fringe malefactors. We know for a fact there have been far-right agitators both online and at these rallies, as well as far-left."

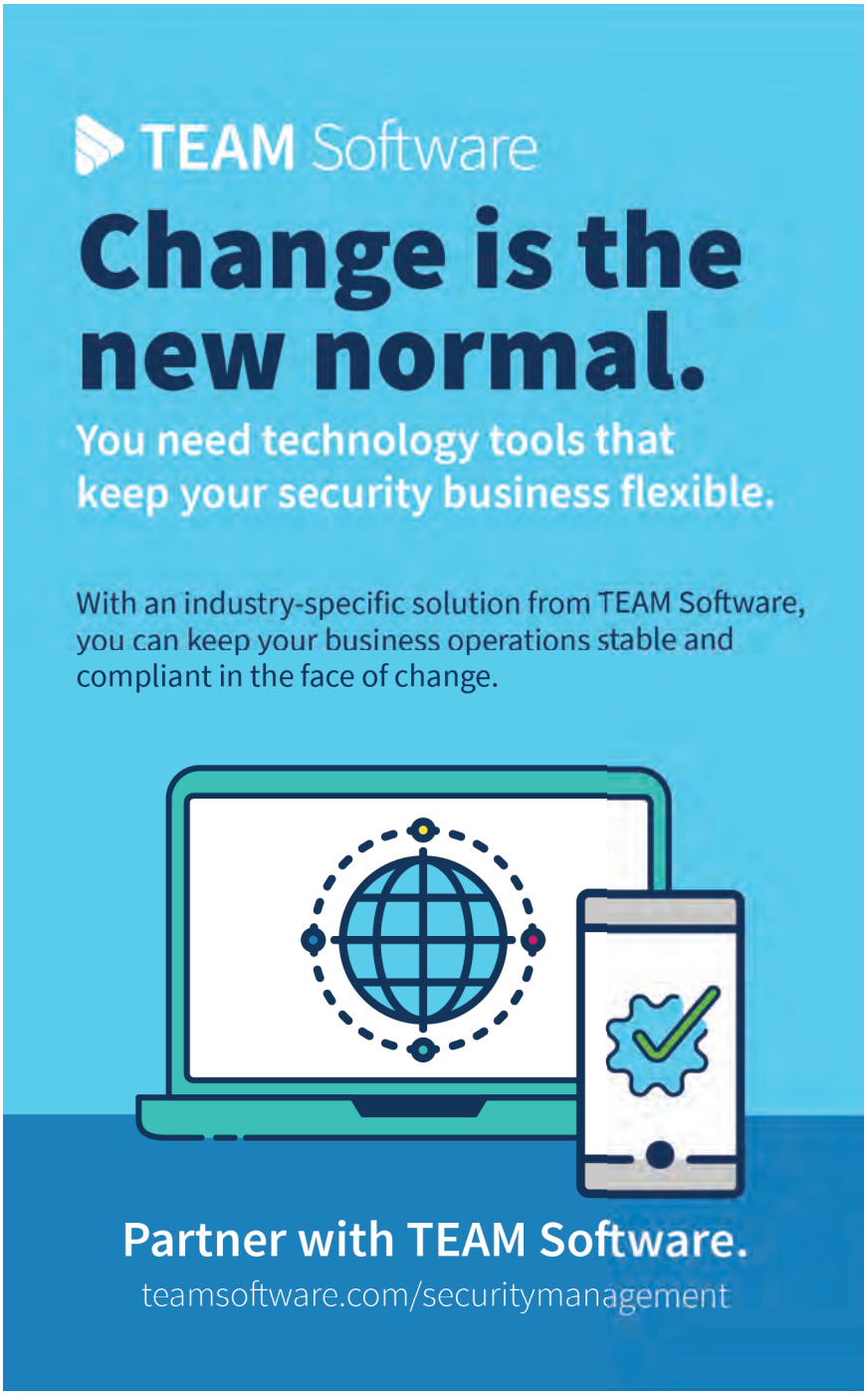
RESILIENCE

Investors and corporations will continue seeking opportunities in the global market. Continuous situational awareness and security trends are as important as a robust business plan for protecting investments in new environments.

As illustrated in this article, there are many global resources available to help in this endeavor for both nonprofit and for-profit organizations. Additionally, ensuring that the C-suite collaborates with finance, investment, planning, and security departments can provide analysis and insights.

Organizations investing further in non-traditional security forecasting abilities will improve their resilience and ensure continued operations in the face of mass disruptions. Traditional physical security will certainly help in protecting facilities and assets. However, analysis and forecasting will better enable an organization's lasting success. Understanding and forecasting evolutions and upheavals in an environment improves the ability to proactively change behavior and practices, instead of reactively slowing or interrupting business operations during mass protests.

Unaddressed economic stressors eventually result in hardship and discontent throughout a population.



For product info #17 securitymgmt.hotims.com

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 CHAIR OF THE GLOBAL TERRORISM, POLITICAL INSTABILITY, AND INTERNATIONAL CRIME COUNCIL.
DIETER ARENDT IS A SECURITY ANALYST FOR THE SOUTH AFRICAN RESERVE BANK BASED IN PRETORIA, SOUTH AFRICA. HE IS A MEMBER OF THE GLOBAL TERRORISM, POLITICAL INSTABILITY, AND INTERNATIONAL CRIME COUNCIL.

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

© 2020 ADT Commercial LLC. All rights reserved. The product/service names listed in this document are marks and/or registered marks of their respective owners and used under license. Unauthorized use strictly prohibited. License information available at www.adt.com/commercial/licenses. 08/20

For product info #18 securitymgmt.hotims.com

A Converged Campaign

With a converged security team, Mastercard is taking a unified approach to addressing risks and educating its workforce to reduce threats.

We are all in this together.

That was theme that swept the world in the wake of the coronavirus pandemic.

The sentiment was reiterated at Mastercard after CEO Ajay Banga released a letter to the financial institution's community, reiterating its commitment to serving its customers, employees, and society as a whole during this unprecedented time.

"At Mastercard, our focus has always been on helping to build a more connected world, and in today's environment, this is more important than ever," Banga wrote. "We remain committed to that cause and are moving forward in a way that supports human safety and global efforts for sustainability now and recovery in the future. We are in this with each and every one of you for the long haul and I am confident that, as long as we keep plugging in to our basic human decency, we will emerge from this and find new strengths and growth we never imagined."

A core component of this crisis response is ensuring that Mastercard employees are safe and can continue their work securely, Banga added.

"During this time of uncertainty, we pledged to all our employees that there will be no layoffs related to the COVID-19 crisis in 2020," he wrote. "And we've initiated several temporary policies according to guidance from regional authorities, international health organizations, and our employees' own concerns and comfort levels, including working from home, split working schedules, restricted or postponed travel, among others."

This approach models a philosophy held at Mastercard that safety and security are not just the responsibility of the security department, but of all employees who play a valuable role in protecting the organization's assets, says Ron Green, chief security officer for Mastercard.

"In the past, the organization would have felt that the security team takes care of that—we have other stuff to do," Green explains. "Today, security is something that we all have to do at Mastercard."

Security Philosophy

Corporate security leaders have discussed the idea of converging their physical security and cybersecurity teams for more than a decade. Roughly 25 percent of organizations in certain parts of the world have taken that step—sometimes also including business continuity—according to research by the ASIS International Foundation, *The State of Security Convergence in the United States, Europe, and India*.

The benefits of this approach include greater ability to align security strategy with corporate goals, greater communication and cooperation, more efficient security operations, and more visibility and influence with the board and C-suite, according to the report.

Mastercard has merged its physical and cybersecurity teams to better address threats that the financial institution faces.

"Our adversaries, they don't think that way—cyber and physical being separate—they just attack," Green tells *Security Management*. "They don't have that artificial boundary to hold them or slow them up. They don't care. Because we're combined, we just think about security."

Other organizations are coming to a similar conclusion—especially when it comes to preventing fraud. For example,

ILLUSTRATION BY *SECURITY MANAGEMENT*; iSTOCK

the U.S. Secret Service recently merged its Electronic Crimes Task Forces and Financial Crimes Task Forces into a single network known as the Cyber Fraud Task Force.

"Online payments and banking are now globally pervasive, credit card numbers and personal information are illegally sold on the Internet and Dark Web, and cryptocurrencies have become one of the primary means by which criminals launder their illicit profits," the Secret Service said in a press release. "No longer can investigators effectively pursue a financial or cybercrime investigation without understanding both the financial and Internet sectors, as well as the technologies and institutions that power each industry."

Mastercard benefits from having a CEO who buys into the philosophy of convergence, Green says. Along with being the CEO, Banga is the co-founder of the Cyber Readiness Institute, served on U.S. President Barack Obama's Commission on Enhancing National Cybersecurity, and led discussions at the Business Roundtable on security matters. Banga's interest in security—and in making it a core component of Mastercard's mission—has helped Green and his team receive buy-in from other executives for their work.

Green briefs the executive leadership team on security threats and provides data about risks to their specific teams.

"The ability to report on the status of their teams' susceptibility, that gives the executives data to go in and talk to their teams," Green says. "If you want to get your executives engaged, you have to make them knowledgeable and provide them with how they can help."

These actions have also encouraged the mind-set that security is everyone's responsibility at Mastercard—not just the security team's domain. This has become especially critical in recent years as social engineering and phishing have become some of the main attack methods for malicious actors to infiltrate organizations and compromise networks. (See "A Patrol Problem," *Security Management*, August 2020)

"One of the principal reasons we're focused on security as everybody's responsibility is if you look at the way the threat moves, many breaches today start from compromising an unintentional insider through phishing and social engineering them to do the wrong thing," Green says. "Companies are then compromised, and data is stolen or altered. But it starts with people not being focused on security."

Raising Awareness

Not everyone is a security expert. But all employees have some degree of access to corporate networks and sensitive data that if compromised could place the organization at risk. All employees need to have some basic security knowledge and receive training to help reduce risk, Green says.

To help educate the general workforce, Mastercard created its Secure It awareness program that focuses on one topic each month. The overarching themes and programs are developed in house, but Mastercard works with a video company to produce sketches that are then shared through its Secure It TV programming.

> *Because we're combined, we just think about security.*

"It's got a usual host of characters that people have become accustomed to handling a security issue, such as connecting to Wi-Fi in a coffee shop or managing passwords," Green says.

Secure It also brings in outside speakers, such as Frank Abagnale, who operated as a con man from the time he was 15 until caught by authorities at age 21 and whose story was dramatized in the movie *Catch Me If You Can*. He later worked for the U.S. federal government and is now a security consultant for the FBI academy and private organizations.

These speakers share information on high-profile security topics, as well as security risks that impact employees' everyday life—such as how to secure your home Wi-Fi network like a professional.

"We do a lot to bring it home," Green says. "If someone tries to trick you into giving up information, or breaking into networks, that puts you and your personal information at risk. We gear up people to think about security in their everyday home life."

The security team also partnered with human resources and communications to help articulate and explain technical concepts to a nontechnical audience, says Neil Parker, Mastercard's business security officer, employee digital experience, and member of the ASIS International Young Professionals Council.

"The technical guys are never going to articulate it in a way to change the mind-set—this is where we need HR, communications, operations, and others to help out," he adds.

Additionally, Mastercard conducts regular phishing training and test campaigns. Mastercard previously only ran these campaigns twice a year, but recently began conducting them every month for all employees—including the CEO and his direct reports.

"We've established standards around acceptable behavior, and there is training if you fail the tests," Green says. "There are also consequences associated with it because our employees are accountable for their conduct. We have a 'three strikes and you're out' policy."

In his monthly briefing with the CEO and senior executives, Green will share the results from previous phishing exercises so they can take that data back to their teams.

"Those executive leaders talk to their teams about the importance of paying attention, having the right hygiene when it comes to protecting Mastercard," Green says.

This became especially critical as many Mastercard employees made the transition to working fully remote during the coronavirus pandemic. In March and April, Mastercard briefly paused its phishing tests to employees. It also beefed up briefings and

information for employees to help them secure their new home office space and help reduce risk to Mastercard.

"With the pivot to put everybody at home, the threat landscape changed," Green says.

Through a Secure It challenge, Mastercard provided videos on securing home routers, things to consider when using an Alexa or Google Home system, and more. Employees who participated in the challenge received a pin for their efforts, and Green says that the voluntary program has caught on.

"I think the transition has been easy for us," says Parker. "We never wanted to look at just security within our walls but security being a way of life. We enable our employees to connect to work from everywhere. You need to be thinking about security everywhere, as your normal way of life."

Programs like Secure It have helped employees see the security team as a business enabler instead of a police force for the organization, Parker adds.

"When we look at legacy and how to get employee buy-in, the big change for corporate security is not being seen as policing the organization," he explains. "We've helped lead the way with that by combining the cyber and physical teams, and by doing that, it's changed us from being the police to being a partner and business enabler—expediting buy-in."

And these programs have helped to make a difference in protecting Mastercard. Banga issued an ambitious goal to the security team: reduce phishing attempt click-through rates to a 1 percent average across the organization. After testing nearly every month, Parker says Mastercard is very close to meeting that goal—despite increasing the difficulty of its testing.

Mastercard is also sharing its best practices with smaller and medium-sized businesses that cannot afford a security apparatus as robust as its own.

"We partnered with the Global Cyber Alliance and created the Cyber Readiness Institute to help provide best practices for small and medium businesses," Green says.

Mastercard has also made tools available to help smaller organizations think through core security components, such as asset management, anti-malware, and network scanning.

"We give you the why of why you need to do it, and also provide videos and free tools so you can manage your assets," Green explains. "We're giving you the ability to raise the game and protect yourself."

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

LIVE EARTH

A Real-Time Awareness Platform to Increase Safety & Security

Visualize Multi-Layer Correlations and Non-Obvious Correlations in Real-Time from a Single Screen

Increase Safety

Easily monitor all of your data sources from a single screen to increase the safety and security of all assets - people, places, and things.

Increase Security

Quickly detect fraud ring activity with real-time notifications of an increase in transaction rates across data sets and regions.

Data Source Examples:
Video Management Systems
Alarms & Access Controls
Physical Locations & Indoor Mapping
Transaction Data
Social Media
Asset GPS & Personnel RFID
Flights
Public Transportation
Weather & Lightning
Drones
Traffic Flow
Accidents & Construction

www.liveearth.com/demo

Trusted by Organizations & Agencies Around the World

For product info #19 securitymgmt.hotims.com

THE POWER OF CONNECTION

Industry Education You Won't Find Anywhere Else

Earn up to 25 CPEs while gaining insight at a time when the security profession is in demand more than ever before. Create your own schedule or follow one of our tracks:

Digital Transformation & Information Security

ESRM

Leadership & Managing Organizations

National Security

Physical & Operational Security

Risk Management

A thriving marketplace of the latest industry technologies and solutions

The GSX+ exhibit marketplace offers a complete showcase of newly-released products and services, complete with in-depth profiles, live and recorded demos, and downloadable content.

*25 CPE credits available per all-access pass.

GSX+
GLOBAL SECURITY EXCHANGE PLUS

Genuine Connections in a Virtual Experience

Don't let your screen hold you back – GSX+ will help you build your network conveniently from your home or office.

- **Secure, AI-driven matchmaking technology will connect you with fellow attendees and exhibitors.**
- **Connect with attendees through one-on-one chat or virtual meeting rooms**
- **Schedule meetings with exhibitor representatives**
- **Participate in unique networking opportunities to further your connections**

Your global ASIS community

Get career support at the ASIS Hub – ask questions about certifications and training, and learn about the latest standards and guidelines for the industry.

Through a new platform, GSX+ opens doors to a world of opportunities and answers for professional development and collaboration.

REGISTER TODAY AT GSX.ORG/SM

BITTER PILLS

As drug diversion temptations rise, healthcare facilities face multitiered loss prevention challenges stemming from an opioid epidemic and the effects of the COVID-19 pandemic.

ILLUSTRATION BY STUART BRIERS

Two Chicago pharmacy technicians stole more than 56,000 tablets of hydrocodone—an opioid painkiller—over a 26-month period from 2015 to 2017. The technicians manipulated the pharmacy's inventory system, falsifying records to make it look like the hydrocodone tablets either had not been received from the distributor or had already been dispensed to patients.

The two techs sold the tablets on the black market for approximately $10,800, according to prosecutors. Both technicians pled guilty to one count of conspiracy to possess a controlled substance with the intent to deliver and were sentenced to between one and five years in federal prison.

"When trusted pharmacy employees illegally divert powerful and addictive pain medications for misuse, they put individuals and their families at increased risk for drug dependence and overdose," said Robert J. Bell, special agent in charge of the U.S. Drug Enforcement Administration's Chicago Field Division, in a news release.

Today, in the face of a global pandemic and economic recession, profiting from drug diversion may become more tempting than ever. Increased regulatory and legal risks, the opioid epidemic, and an evolving drug abuse landscape have also made drug diversion and loss prevention a higher priority in the healthcare system than ever before.

Drug diversion programs are designed to prevent the diverting of legally prescribed drugs from their intended medical use to any illicit use. According to the U.S. Department of Justice National Drug Intelligence Center (NDIC), the estimated cost of diversion to public and private medical insurers is more than $72 billion per year.

It is likely that future U.S. government enforcement activities will focus on the responsibility of organizations to prevent drug diversion. If that occurs, those organizations would be liable for the diversion. In anticipation of this shift, best practices have evolved to include a diversion enterprise management emphasis that encompasses a multidisciplinary team approach.

Drug diversion regulatory and legal risks have escalated over the past four years, with a series of sanctions and civil proceedings impacting drug diversion control programs.

One of the high-profile sanctions occurred in August 2018, when the U.S. Department of Justice (DOJ) announced a record $4.3 million settlement with the University of Michigan Health Care System in which the hospital also agreed to correct "system-wide" violations of tracking controlled medicines.

The U.S. Drug Enforcement Administration (DEA) began its extensive audit of the university following two tragic incidents involving a nurse and an anesthesiologist, both of whom overdosed on drugs intended for patients. The U.S. attorney who announced the action noted that the hospital has "an obligation to its patients, to its employees, and to the public to responsibly control its drug inventory."

The risk to patients can be tremendous. In one incident in Colorado, pain medication in the syringes used during surgeries was stolen, injected by a person dependent on opioids, and replaced with saline. Following an investigation, police charged a surgical technician with the thefts. He was found guilty and sentenced to more than six years in prison. The hospital sent notices to more than 3,000 patients that they may have been infected with hepatitis B, hepatitis C, and HIV during their medical procedure at the hospital.

On the legal front, more than 900 U.S. state, local, and tribal governments have a pending suit in U.S. District Court in the Northern District of Ohio against wholesale distributors and manufacturers of opioid pain medications, seeking damages sustained from the opioid epidemic. The suit alleges these companies recklessly marketed prescription painkillers while downplaying the dangers of addiction and death. Some legal analysts predict an eventual settlement could exceed $1 billion.

In August 2019, an Oklahoma judge ruled that drugmaker Johnson & Johnson deceptively marketed painkillers, helping to spark the state's opioid crisis—which claimed the lives of more than 6,000 people in the state. The case was hailed as the first to hold a pharmaceutical company responsible for the epidemic, and the company was ordered to pay $572 million.

The pressures on diversion programs also come directly from America's use of opioid pain medications, which grew exponentially between 2000 and 2019. Some of this growth was due to legitimate prescription use, but a portion of it was also due to abuse of opioids. U.S. National Institutes of Health (NIH) data showed that overdose deaths from commonly prescribed opioids during this period rose from 1.3 deaths per 100,000 people to 5 deaths per

100,000. According to the U.S. Centers for Disease Control and Prevention (CDC), in 2018, more than 46,000 Americans died from opioid overdoses. That translates to approximately 130 deaths per day. According to the CDC, overdose deaths involving prescription opioids were more than four times higher in 2018 than in 1999.

In 2017, the NIH *National Survey on Drug Use and Health* revealed an estimated 2 million Americans misused prescription pain relievers for the first time within the previous year. The CDC found that from 2002 to 2010, there was a 74 percent increase in chronic nonmedical use of opioid pain medications, and 2018 CDC data showed that opioid prescribing rates continue to be high in certain areas of the United States—some counties have opioid prescription rates six times higher than the national average.

When trusted pharmacy employees illegally divert powerful and addictive pain medications for misuse, they put individuals and their families at increased risk for drug dependence and overdose.

The United States is not alone in this crisis: Canada experienced more than 10,000 opioid-related deaths between January 2016 and September 2018.

Opioids are a class of drug with a high long-term dependency risk profile. According to medical and drug abuse treatment professionals, opioid dependency is one of the most difficult addictions to beat, and the struggle can last a lifetime. (See "A Constellation of Challenges," *Security Management*, November 2019.)

An ever-evolving drug abuse landscape in the United States and other countries means there are additional drug diversion challenges beyond depressants (a type of drug that includes opioids). Abuse of stimulants—which include methamphetamine and cocaine—is also on the rise. In 2020, U.S. law enforcement reported unprecedented record seizures of methamphetamine along the U.S. border with Mexico. The DEA reported increases across the United States in methamphetamine purity and decreases in price. Both of these are indicators of increased supply. The CDC has also reported an increase in methamphetamine overdose deaths.

The Canadian Centre on Substance Use and Addiction reports that methamphetamine availability has rapidly increased in Canada. The United Nations Office on Drugs and Crime (UNODC) reported in May 2020 that the price of methamphetamine has dropped to the lowest level in a decade as the supply has surged.

"While the world has shifted its attention to the COVID-19 pandemic, all indications are that production and trafficking of synthetic drugs and chemicals continue at record levels in the region," the UNODC noted.

Meanwhile, the European Monitoring Centre for Drugs and Drug Addiction reported mixed methamphetamine rates, with prices dropping significantly in The Netherlands, Sweden, Hungary, Cyprus, and Austria, while increasing in Croatia, Denmark, Finland, Poland, and Romania.

A 2016 European Union study on opioids found that there was a high rate of prescription pain reliever abuse in the EU, although not as high as in the United States—20 percent for those aged 12 years and over, compared to between 7 percent and 13 percent in the EU.

In 2020, U.S. law enforcement reported increased seizures of cocaine from South America. Maritime seizures of cocaine shipments by U.S. law enforcement are at a level not seen since the 1980s. Europol reports that cocaine trafficking in Europe has been at historical highs, with much of it entering via maritime freight, primarily from ports in The Netherlands, Belgium, and Spain. The signs of increased abuse of stimulants is expected to put pressure on illicit abuse of pharmaceutical stimulants such as Adderall, Dexedrine, and Ritalin.

Additionally, societal pressures and health risks associated with the COVID-19 pandemic are heightening drug abuse and drug diversion risks.

COVID-19 and Drug Diversion

Without question, COVID-19 dramatically increased personal stress on healthcare personnel. Many healthcare workers bore the increased burden of fearing they might become a carrier of COVID-19 and transmit it to their families and loved ones.

In addition, healthcare workers assigned to intensive care units reported tremendous emotional burdens of caring for patients dying of the disease with no family or loved ones by their bedsides. A consequence of increased pressures and occupational stress is greater risk that healthcare workers will abuse drugs as a coping mechanism.

COVID-19 has also significantly disrupted drug treatment programs and facilities. These rely on one-on-one counseling and group therapy. Addiction is a disease of isolation. Both in-patient and out-patient drug treatment programs include soothing human contact such as handshakes, hugs, and other social rituals to build bonds of support.

As a result of shelter-in-place and social distancing orders, treatment programs were forced to transition to Web-based remote counseling efforts. These are not ideal for drug treatment.

A preliminary analysis by the White House Office of National Drug Control Policy showed an 11.4 percent increase year over year in opioid overdose fatalities for the first four months of 2020. The analysis attributed the increase to the impacts of quarantines, lockdowns,

and economic uncertainty impacting the addiction crisis.

Methadone clinics—which dispensed daily doses of medicine to opioid-dependent people in treatment—faced difficulties with social distancing as well. Clinics were authorized to switch to dispensing up to 25-day dosage units at a time for self-administration by patients. In addition, people struggling with drug dependency faced layoffs, unemployment, eviction, social isolation, and other stressors that increase feelings of desperation. These factors have dramatically increased risk of relapse for those suffering from the disease of addiction.

Additionally, as a result of COVID-19 there is increased pressure on diversion control programs. In April 2020, the DEA increased quotas by 15 percent for manufacturing and importation of controlled substances to prepare for an increased demand from patients on ventilators requiring fentanyl, morphine, and codeine. Simultaneously, the ease of access to controlled substances for healthcare professionals was increased. Telemedicine regulations were also eased to make it easier for physicians to prescribe medication to patients without an in-person examination.

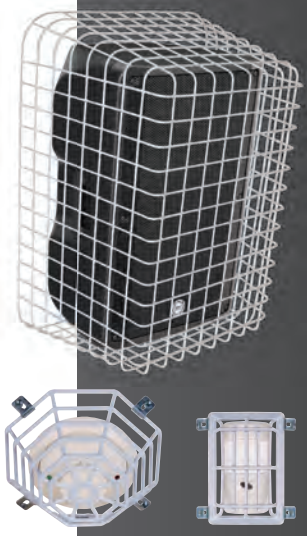
These three actions, while potentially beneficial during the pandemic, also increased the risk of diversion of pharmaceuticals for illicit use. Earlier this year, the National Safety Council (NSC) released recommendations and guidance around COVID-19 associated opioid risk in the workplace. According to the American Medical Association (AMA) in June, more than 30 U.S. states reported increases in overdose deaths. Kentucky estimated a 25 percent increase in overdose deaths as well as a rise in emergency medical calls and emergency room visits related to overdoses. In Cook County, Illinois, suspected or confirmed overdose deaths doubled in the first five months of 2020.

Increased overdose deaths are an indicator of increased drug abuse and demand. These will place further pressures and increased challenges to drug diversion loss prevention programs.

High-Risk Areas

Best practices and risk profiles for drug diversion vary depending on whether the program is for a retail pharmacy, hospital pharmacy, medical clinic, doctor's office, pharmaceutical company, or other entity. Three venues, however, are the more common, reoccurring high-risk areas for drug loss.

Rely on STI®



...to protect against theft & damage

Big or Small, Protect it All

STI has the right wire guard, right now. Constructed of tough, 9-gauge steel wire coated with corrosion resistant polyester or cold-rolled steel. Many models available to protect against damage.

- Offers protection for vulnerable devices of all sizes
- Prevents vandalism, damage, misuse, and theft
- Super tough construction
- Fast and easy installation
- Custom cages available

Learn more at www.sti-usa.com/sema149
or call 248-673-9898

2020

STI 40 YEARS Safety Technology International

For product info #21 securitymgmt.hotims.com

Brick-and-mortar pharmacies. We all know the old phrase in murder mysteries: "The butler did it." In any retail pharmacy practice, the same association holds true for loss of controlled substances and pharmacy technicians. In many instances, when there is a loss of drugs in a pharmacy, a pharmacy tech is responsible.

Another high-risk area for diversion in any pharmacy is "returns," a term for drugs that are expired or have been recalled and are stored pending return or transfer to a distributor for destruction. When proper controls are not in place, returned controlled substances are at high risk of theft. These drugs should be inventoried and kept secure in a locker or safe until their transfer.

"If you see something, say something" is as important to any drug diversion program as it is to antiterrorism initiatives.

A third major risk—secure record keeping systems and cybersecurity—was identified during the mass protests in the United States throughout May and June 2020, when brick-and-mortar pharmacies nationwide became targets for looters who carried out large quantities of prescription drugs. Drugs used to manage abuse, which can also be abused, were popular targets, as were stimulants such as Adderall.

In Philadelphia, 180 of the city's 476 retail pharmacies were broken into and looted; Philadelphia Police Department investigators believe the pharmacy attacks there were strategically planned.

At some locations, in addition to stealing the narcotics, looters hauled away the computer systems the pharmacists used to maintain the inventory audits, making it difficult to ascertain what medications were stolen, and complicating pharmacies' regulatory compliance reporting of drug theft.

Hospital pharmacies. Hospital pharmacy practices carry many of the same risks of a retail brick-and-mortar pharmacy, with two additional significant risk areas. One is Automatic Dispensing Machines (ADMs). The second is the liquid drugs and syringes used daily throughout the hospital. Both are the most common areas in a hospital where drug diversion occurs.

ADMs are the medical equivalent of ATMs and should be treated as such. Access and policies should be up to date, and usages should be reviewed at least weekly by supervisory personnel.

Syringes containing powerful opioids are an important and daily tool in a hospital, but they need to be kept secure before and after their use through policies that limit access before use and "rule of two" wasting at their completion. The rule of two mandates that at least two people be physically present to conduct, witness, and certify the activity. Having a second person present is intended to decrease opportunities for theft.

Medical personnel across the country continue to divert syringes containing opioids for their own illicit personal use, usually in the minutes before and after their legitimate use.

In December 2019, a nurse at the University of Colorado Hospital was sentenced to U.S. federal prison for stealing opioids by deceit and tampering with a consumer product. She used her access to ADMs to steal opioids intended to treat patients. She used a syringe to self-inject the fentanyl and hydromorphone in a hospital bathroom, refilled the medicine vials with saline solution, and placed them back into the ADM.

Medical clinics. Medical clinics that do not store drugs generally carry low risk except in one area: access to the medical provider's paper or electronic prescription pad.

Oftentimes, an employee of the office will either fraudulently prepare a paper prescription, telephone in a fraudulent prescription, or—if he or she has access—submit a fraudulent prescription electronically.

For example, in May 2020, a medical office manager in Buffalo, New York, pled guilty in U.S. federal court to issuing or causing 116 fraudulent hydrocodone and oxycodone prescriptions over a three-year period without a physician's authorization.

The manager accessed the physician's prescription pad and a New York State-issued controlled substance electronic prescribing hard token and passwords. He then filled the prescriptions, issued in the names of associates and fictitious individuals, from various pharmacies in the region. The scheme was discovered when a suspicious pharmacist, who questioned the legitimacy of a prescription, contacted the physician.

It is extremely important that providers recognize these possibilities and always secure their paper prescription pads, never share their electronic passwords, and routinely review their prescribing history at least quarterly for any abnormalities.

Management and Culture

The best drug diversion loss prevention efforts today are comprehensive programs with separate, yet equally important, components synched into an enterprisewide undertaking. These vary by the type of entity being safeguarded. For example, most hospital in-patient pharmacy programs will include a focus on drug procurement, storage, dispensing, return, and disposal; physical security; surgical areas; physician prescribing; and nursing care usage.

The programs also feature multidisciplinary resources to tackle the mission. A diversion program manager

now routinely works in concert with a security manager, legal, management, IT, a pharmaceutical specialist or team member, and a head nurse. This approach is critical to synthesize unique technical knowledge, expertise, and perspectives to quickly eliminate anomalies that have legitimate explanations and then immediately focus program resources on red flags that require quick mitigation actions.

An organization's drug diversion culture is key to its success. Studies from various sources, including *The American Journal on Addictions*, show that 10 to 15 percent of healthcare workers are at risk of substance abuse. These are the personnel who pose great risk to the illicit diversion of pharmaceutical drugs.

That means that the overwhelming majority of workers—the remaining 85 to 90 percent of employees—can be recruited to serve as the first line of defense to protect the organization and its patients from risks of drug diversion. These professionals can be educated on what kinds of coworker behavior may be indicative of drug dependency. In a 2020 Porter Research survey of healthcare executives, 75 percent reported that their organization used diversion awareness programs, and of those, 85 percent reported that their program includes employee tips on suspicious activities.

There are many indicators of opioid pain medication abuse, and their value increases with the presence of each additional indicator. Examples include repeated failure to fulfill work and educational obligations; falling asleep in vehicles, at workstations, or in restrooms during breaks; and withdrawal from social, recreational, or professional activities. Physically, pinpoint pupils are indicators of opioid intoxication and overdose; dilated pupils are indicators of opioid withdrawal. Other indicators of withdrawal include nausea, restlessness, cramps, sweating, runny nose, watery eyes, and mood swings.

"If you see something, say something" is as important to any drug diversion program as it is to antiterrorism initiatives.

Monitoring and Surveillance

Over and over again, failures in monitoring and surveillance regimens have surfaced as weaknesses in drug diversion programs. The strength of these systems will determine how well irregularities are ferreted out and flagged for appropriate action. Monitoring and surveillance is the primary role of diversion program managers.

One recent DEA investigation in Cook County, Illinois, highlights this problem. Criminal investigators were contacted by relatives of several elderly patients who had been receiving long-term care from a physician who specialized in caring for homebound seniors. Many of them had mobility issues, making trips to doctor's offices difficult.

The patients' relatives reported they became suspicious of the types and amounts of medications being prescribed for their loved ones. When investigators conducted interviews and examined records, their attention quickly focused on the physician—a reputable doctor who had been conducting in-home care for more than a decade.

With the consent of cooperating victims, investigators installed hidden cameras and microphones in their homes. Soon thereafter, while making rounds, the doctor was captured repeatedly on video stealing pills from patients' prescription bottles. Investigators established the physician was prescribing opioid pain medications to her senior patients that they did not need and could not afford. During her visits to their homes for examinations, the physician would distract the patient, often asking them to retrieve an item in another room, while she emptied pills into her pockets.

While this may sound like petty crime, the doctor had hundreds of patients, and the illicit street value of drugs being regularly stolen was significant. Had proper monitoring and surveillance systems been in place, the physician's irregularities would have been quickly identified and flagged by the medical provider, pharmacy, and healthcare providers.

All U.S. states, except Missouri, now have statewide electronic databases that require medical providers to track prescriptions with the potential for abuse. These allow pharmacists and doctors to see a patient's prescription history so they can identify and flag for action an irregularity that may indicate a disease of addiction.

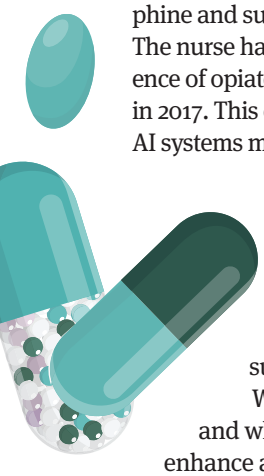
Partnering with Artificial Intelligence

Artificial intelligence (AI) is now a critical partner and best practice in drug diversion programs.

In all risk mitigation strategies, the steps are the same: identify, assess, and mitigate. The strategy is a failure from the start when identification does not occur. A recurring issue in drug diversion programs is effectively using limited resources to ensure potential risks are initially identified. This is a function of monitoring and surveillance—AI blends the talents of IT, diversion program managers, and healthcare experts.

AI uses algorithms to help identify higher-risk medications and higher-risk dispensing patterns among healthcare personnel. Some of these software programs use risk-scoring formulas that combine data from physically tracking drugs in the supply chain, patient medical records, and behavioral analyses of healthcare staff. These programs also quickly spot outliers and alert security personnel. The program could help personnel catch whether a hospital pharmacist dispensed a drug when they were not working or if a nurse or technician signed out a drug at 9:00 a.m. but disposed of it at 2:00 p.m.

In June 2020, a registered nurse at a nursing and rehabilitation facility in Massachusetts pled guilty in U.S. federal court to diverting and diluting morphine sulfate from patients, including an 89-year-old hospice patient. The nurse extracted the medication from bottles



and replaced it with other liquids. The hospice patient received diluted morphine and suffered unnecessary pain. The nurse had tested positive for the presence of opiates during a drug screening in 2017. This case is an example of how AI systems might have prevented drug diversion by identifying the nurse's history as higher risk and worth additional scrutiny before granting access to or administration over highly addictive substances.

While AI is a force multiplier and when used effectively can enhance a monitoring and surveillance system, an experienced response team is essential to analyze the data, look for gaps, and conduct follow-up investigations where appropriate. AI must never be considered a replacement for monitoring and surveillance. AI-enabled software is only as good as the diversion program manager, security manager, and personnel who make decisions based on the information provided. The best program will have no value if security staff are not acting on it.

Audit, Audit, Audit

Internal audits are the lifeblood of successful drug diversion programs. One of the most important functions of an audit is to independently evaluate how well diversion managers are monitoring and surveilling. They also provide reviews of compliance with federal and state regulations and internal policies and procedures. Importantly, audits will also assess the quality and completeness of the diversion investigations conducted.

The comprehensive audit function includes everything in the lifecycle of controlled substances, from the beginning step in procurement through disbursement or disposal. In procurement alone, there must be audits of the use of the Controlled Substance Ordering System (CSOS), separation of duties between those who order and receive the order, signatures of witnesses upon receipt of orders, verification of licensed registrants in the process, validation of the chain of custody procedures and documentation, quarterly review of purchases against inventory, and examination of compliance with purchasing in unit dose packages. An audit system—done correctly—will highlight any instances of noncompliance and identify opportunities to improve systems and procedures to the attention of managers.

Independent, third-party audits of diversion programs are highly recommended because they provide assurance and recommendations by an objective, external set of eyes that evaluate the organization's diversion program. These should include a review and assessment of policies and procedures, controls, monitoring, enforcement, and internal improvement processes. Audits should also include evaluation of HR practices, substance abuse policies, employee drug abuse awareness programs, supervisor training, drug diversion program employee training, and employee discipline for diversion violations.

Trusted Partners

While an outside perspective of drug diversion and loss prevention plans is helpful, organizations sometimes engage physical security consultants who fail to include regulations—such as Title 21, Code of Federal Regulations (CFR) requirements in the United States—in their final assessment and recommendations. It's one thing for security experts to provide physical security expertise, but with facilities handling controlled substances, employed experts should be versed in the federal regulatory requirements (CFR 1301.72) for pharmacies, narcotic treatment programs, drug storage areas in clinics, doctors' offices, medical facilities, and manufacturers. This industry-specific knowledge and experience can produce significantly different guidance from general security practices.

For example, minimum security baselines for a U.S. pharmacy handling schedule I and II controlled substances will differ greatly in cost and sophistication depending on whether it was constructed before or after 1 September 1971. There are many family-owned independent pharmacies scattered across the United States that have been in business for decades—housed in older buildings with simple steel door vaults, a combination or key lock, and an alarm system—that fully comply with the CFR.

For any vault facilities constructed after 1 September 1971, however, there are rigorous specifications that must be met to be compliant with the CFR. For example, the walls, floors, and ceilings of the vault must be constructed of at least eight inches of reinforced concrete or other substantial masonry, reinforced vertically and horizontally with half-inch steel rods tied six inches on center, or the structural equivalent to such reinforced walls, floors, and ceilings. Similar specific requirements relate to the door and frame, day gate, and alarms.

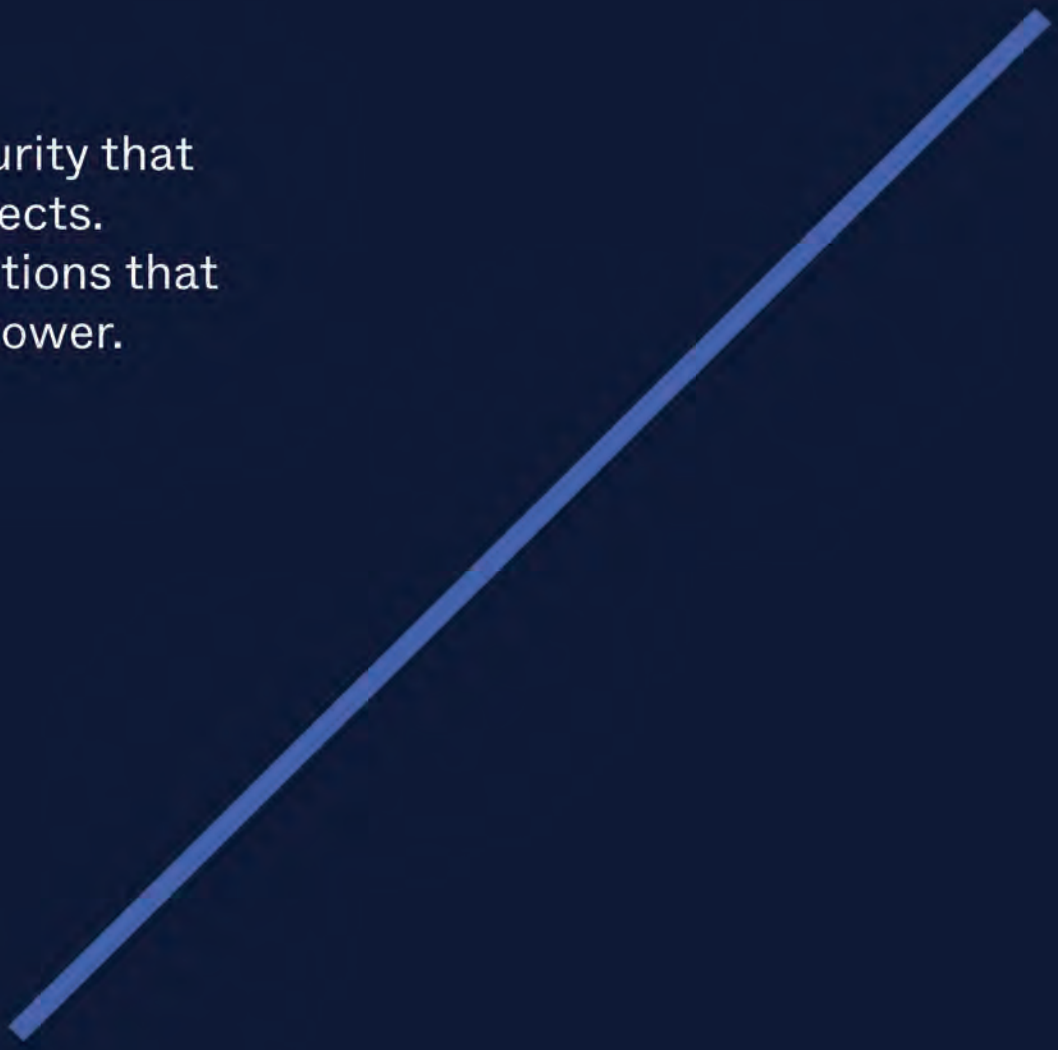
Paying for drug diversion loss prevention consulting services needs to be about the right kind of experience and knowledge. Without the necessary background information and experience, a consultant might recommend investing in expensive security measures for compliance issues that do not apply to the organization.

The effects of COVID-19 help to illustrate how one event can have enormous impact on organizations and programs. The pandemic also underscores the importance of adjusting and reacting to ever-changing and complex threats.

Continual security and threat reviews, coupled with strong flexible policies, regularly occurring training and audit programs, and an organizational culture that requires its professionals to embrace knowledge and change will put drug diversion loss prevention leaders in position to fight this crime. ■

MARK GIUFFRE, CPP, CFE (CERTIFIED FRAUD EXAMINER), CAMS (CERTIFIED ANTI-MONEY LAUNDERING SPECIALIST), IS A DIRECTOR AT SECURITY RISK MANAGEMENT FIRM HILLARD HEINTZE, A JENSON HUGHES COMPANY, WHERE HE SUPPORTS CLIENTS IN INVESTIGATIONS, SECURITY, AND LAW ENFORCEMENT CONSULTING.

Security that protects. Solutions that empower.



ZBeta designs for what you want to achieve, not just what you want to protect.

ZBETA

www.zbeta.com

For product info #22 securitymgmt.hotims.com

Virtual Vetting

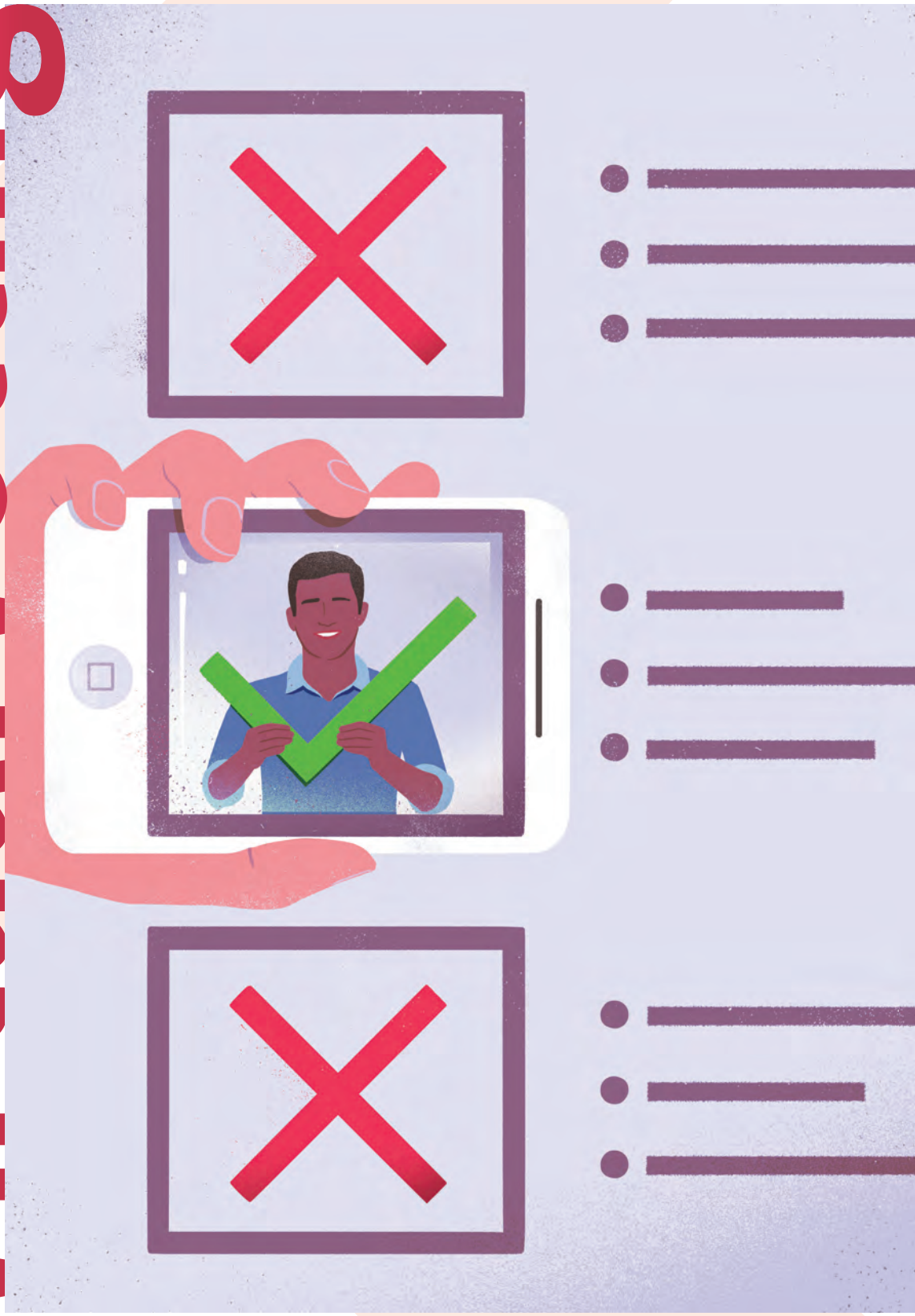


ILLUSTRATION BY SÉBASTIEN THIBAULT

Emerging technology, changing client demands, and multigenerational staff management were already changing the hiring process for security staffing companies. Then COVID-19 came along.

How do you hire from a distance? Office closures and social distancing measures brought on by the COVID-19 pandemic have forced the contract security guarding industry to change how it recruits, evaluates, and hires new personnel, and while many changes are temporary, others can present long-term opportunities for improvement.

Over the last decade, the contract security industry has seen marked changes in both the applicant pool and the officer skill sets required by customers. A more recent development has been interviewing and conducting applicant processing and onboarding remotely as much as possible.

In particular, the 2008 financial crisis changed the landscape for security talent management. While many industries faced setbacks, the recession presented unexpected benefits for contract security companies.

From 2008 to early 2017, hiring for security firms was a straightforward activity in the United States. Given the generally high but stable unemployment rate and slowly growing economy, the labor pool was both diverse and plentiful. It was not uncommon for a security officer applicant to have substantial life experience or college degrees. The stability of the security industry offered steady employment, albeit rarely at an individual's prior salary range. Turnover—always an issue in most service industries—tended to be more manageable; keeping a job often trumped seeking a new job.

During this same period, technology finally found its way to contract security. Unprecedented industry consolidation, driven by a wave of retiring owners and uncertainty with the U.S. Affordable Care Act, led national and international firms to differentiate themselves through technology and service. This, however, required a different level of security officer skill set.

21st Century Skill Sets

One important area of service that has fundamentally never changed in the contract security field is that security personnel are expected to show up when and where they were supposed to, look the part through uniformity, understand their responsibilities, be prepared to document both the routine and the extraordinary, and know the right person to notify when necessary.

However, the sophistication level and visibility required of today's security officer stands in stark contrast to what was needed just a few short years ago. Primarily, the evolution has centered on the demand for more extensive training and the ability of each officer to perform, communicate, and respond professionally in a seemingly ever-growing range of safety and customer service-related areas.

Customer expectations for proficiency have never been greater. Security officers must be prepared to control access, welcome important guests and escort each to their destination, interact with local law enforcement, lead evacuations, respond to medical emergencies, de-escalate tense situations, and mitigate risk.

Technology tools and the skills to use them efficiently have become the industry standard, with a goal of maximizing officer performance and collecting risk management data. Today's security officer is searching for and locating

potential threats, while controlling access using technologically advanced surveillance systems. Routine security officer functions now include electronic incident reporting, camera monitoring, and collecting patrol tour data, which is accessible in real time.

Security companies have also created online programs to make training more accessible, markedly enhancing the skills and knowledge of each officer. Professional security officers now actively pursue computer skills and additional training as a path to upward mobility.

Multigenerational Hiring

Between 2016 and 2018, numerous industries that had been idling during the recession reentered the hiring competition with gusto. For contract security firms, educated and experienced applicants seeking employment and stability evaporated. The trouble was: prospective and current clients' service needs had not evaporated in the slightest.

Veteran hiring, long a panacea for security firms, was in vogue. As the Iraq War wound down, veteran recruitment became a highly publicized hiring initiative in multiple industries, substantially reducing a crucial and previously consistent security industry employee base. Compounding this challenge, many mature men and women retired or left the workforce. This senior applicant pool, a critical part of the infrastructure of a stable security company, couldn't be replaced in anywhere near the numbers needed. Suddenly, almost every conversation between industry executives centered more around recruitment, hiring, and retention than any other managerial obstacle.

> The sophistication level and visibility required of today's security officer stands in stark contrast to what was needed just a few short years ago.

With this evaporation of veterans and mature candidates, the era of the millennial security officer arrived and with it would come a bushel full of new generational challenges.

Recruiters and talent management experts have devised many strategies for attracting and retaining highly educated millennials—an age range that generally includes people born between 1981 and 1996. Most of these recruitment efforts emphasize values alignment, flexible schedules, being tech savvy, and

For product info #23 securitymgmt.hotims.com

We're proud to welcome Tony York, one of the foremost healthcare security experts in the world, to the PalAmerican Family.

At PalAmerican Security, we're continuing to grow even stronger in how we deliver for our clients with the addition of Tony York to our team as Executive Vice President. With an incredible track record of developing and strengthening security programs, Tony brings over 25 years of experience, leadership and expertise. Well-known for being an engaging and influential leader in the healthcare security field, Tony co-wrote the book Hospital and Healthcare Security, and holds both Certified Protection Professional (CPP) and Certified Healthcare Protection Administrator (CHPA) designations. Welcome to the team, Tony.

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 #24 securitymgmt.hotims.com

personal investment in the work. The true question for the private security industry, though, was how would the strata of entry-level, hourly millennial service workers fare?

Security hiring has commonalities and stereotypes. Previously, successful job applicants arrived on time or a few minutes early for an interview, were polite to the receptionist, dressed up for the opportunity, and seemed generally interested in the job for which they were applying.

However, the tight labor market changed the caliber of job applicants, especially for entry-level jobs. Suddenly the average applicant exuded an air of boredom and disinterest. Tattoos, piercings, and colored hair went from rare to common.

During interviews, staffing specialists faced conflicting demands—a need for officers and a group of applicants that refused to work for the rates offered. Pay and billing rates—many of which had remained unchanged or barely affected since late in 2008—now faced strong upward pressures. Heightened demand for frontline guarding services during the pandemic only made recruiting and training qualified candidates more challenging.

New Efficiencies

The mission during COVID-19 was to reduce time spent "in the office" during processing in every imaginable way possible, including while recruiting and hiring security personnel. Technology provided solutions.

The year 2020—due to more modern software, cost-effective access to video, and the need to minimize in-person interaction—will probably be seen as the inflection point when security officer processing became primarily remote. Fully remote processing may currently be a bridge too far, but the groundwork for continuing these trends lies before us. When necessity dictated the change to remote employee processing, the industry responded quickly.

Recruitment. Recruiting today barely resembles the version of just a decade prior. Long gone are the days of newspaper advertisements.

Advancements in job posting sites have seen many come and go, and sites are constantly jockeying for position. For example, Indeed.com is currently the "king of the hill" for security officer job listings, given that LinkedIn and Monster.com have generally focused on white collar applicants. Glassdoor is seeking to transition from a place for employees and applicants to complain about employers to a more well-rounded employment platform.

Social media advertising is inexpensive and can be targeted, but it comes with the vitriol that even seemingly random commenters care to tag ads with—editing comment sections is a new but essential task for human resources.

History tells us that once the waters recede, the pluses of non-present interviewing will lead to even more widespread adoption.

Remote interviewing. After the onset of the COVID-19 pandemic, organizations worldwide were almost immediately affected by the requirements of social distancing and limits to the number of people in an office. Human resources departments converted almost instantly to the various video platforms, and screeners sought to maximize video conferencing tools to visually observe applicants and their mannerisms.

As the author's company pivoted to remote interviewing, Erica Montoya, the firm's human resources director, found that the crucial components of an in-person interview, such as punctuality, attentiveness, and overall effort into being ready for a job interview were still applicable. Her team of staffing specialists readily agreed. Each had stories of exceptional applicants who interviewed well, along with funny tidbits—including an applicant who commenced baking brownies during the interview.

These changes may have implications beyond the duration of the pandemic. Several aspects of winnowing the applicant pool had already lent themselves to modernization, such as applying through an employee portal, often with a "screening" function in the process separating the potential successes from the likely failures. Other efficiencies, such as a secondary six to eight question screening phone call, will most likely fold into the video interview.

Dr. Benjamin Dobrin, dean of the D. Henry Watts School of Professional Studies at Virginia Wesleyan University, believes that wholesale commitment to distance interviewing—while born out of the necessities of the pandemic and associated social distancing precautions—will likely remain in effect long-term.

"This has been a jump start, if you will, for businesses still practicing traditional hiring techniques," Dobrin says. "Those that have been slow to embrace interviewing technology were just forced to make a quantum leap. History tells us that once the waters recede, the pluses of non-present interviewing will lead to even more widespread adoption."

Paperwork. In early March 2020, there were a few variations in how traditional hiring paperwork was completed. Across the United States, some security officer candidates arriving for processing started their day with a clipboard, a pen, and the usual suspects: I-9s, tax forms, and handbook acknowledgments.

Fast-forward a few short months, and the clipboard is all but obsolete. Software that captures digital signatures eliminates touching shared objects like pens, and it means paperwork can be completed in the safety and comfort of one's home. Doing so reduces risk and potential exposure to both the processor and new employee, and it carries the inherent message that the organization

HIGH PERFORMANCE
CELL PHONE, WEAPON AND CONTRABAND DETECTORS

- **FULL-HEIGHT DETECTION**
- **ADVANCED TECHNOLOGY, COMPACT DESIGN**
- **EXTREMELY DURABLE & RELIABLE**
- **COVERT ACCESS CONTROL CAPABILITY**
- **APP FOR MONITORING DEVICE, SETTINGS ADJUSTMENT & DATA LOGGER DOWNLOAD**

THE CEIA DIFFERENCE

- The standard for safety, convenience and accuracy
- Superior detection and throughput
- High discrimination of non-threat items with EVO configuration
- Unmatched reliability

ferromagnetic@ceia-usa.com
WWW.CEIA-FMD.COM

CEIA® USA
FERROMAGNETIC DIVISION

For product info #25 securitymgmt.hotims.com

cares about its employees and their health, which is definitely a sound message to have ring out loud and clear to people joining the team.

The transition was not without its challenges. Multigenerational employment pools communicate very differently. Montoya and the processing portion of her team found themselves revising flow charts to account for remote processing tasks. Email was the only effective method for detailing what items needed to be completed remotely, as well as what identification documents must be brought for the inter-office visit.

The trouble with email, though, is that not all applicants check it regularly, with reasons frequently split along generational lines. To mitigate the risk that essential tasks might go unread, mature candidates receive phone calls reminding them to look for emailed processing task lists, whereas younger applicants receive text message reminders.

Training videos. Across the security industry, the spectrum of pre-assignment training videos had often been limited to an office-provided terminal with a VHS tape, DVD, or Web link, usually supervised to ensure that materials were viewed and comprehended.

A mass migration towards providing pre-assignment subject matter remotely has been aided by two developments. First, content can be set up so that it cannot be fast-forwarded or skipped, but otherwise employees can learn at a pace that works for them. This eliminates the concern of "pencil whipping" information that is important for officers to know: attention to detail, customer service, daily and incident report writing, and the use of force continuum.

The second benefit of remote viewing is the ability to embed quiz questions throughout the subject matter or as a comprehensive final quiz. Failure—either because the applicant was unable to absorb the content sufficiently or not paying attention at all and winging it—is a strong indicator that a person is destined to fail in their role as a security officer. For these reasons, completing videos remotely easily passes the test for streamlining processing.

Orientation. Few things can match being welcomed in person with a clearly delineated list of expectations and responsibilities, the chance to meet coworkers, a comfortable environment that invites questions and feedback, and the opportunity to rub elbows with the company's support staff.

Social distancing and infection mitigation pushed this type of orientation into the realm of "the way we used to do it." Blessedly, with so many meeting software platforms, a combination of prerecorded and live orientation material can accomplish much of the same goals at a substantially reduced risk.

Uniforms. Paperwork, pre-assignment videos, and orientation lend themselves much more easily to software and remote technology than the age-old process of issuing uniforms. When an officer visits the office to pick up his or her uniforms, even after calling ahead to a uniform room manager with sizes, it makes the most sense to have the officer try the items on then and there.

We are living through arguably the most accelerated amalgamation of technology and public health concepts in human history.

If an in-person office visit is required, the employer can maximize the officer's visit by completing any additional tasks—such as providing an actual copy of the Employment Handbook and the employee's first weekly schedule, confirming healthcare choices or dependents on tax forms, and meeting the account manager in person—in one short, concise session.

History shows us that times of great strain and upheaval often end up being catalysts for marked change, and for the private security interview and hiring process that adage has proven true. It is doubtful that even a partial regression will occur after COVID-19, given the ease and efficiency of digital interviewing and the degree to which it highlights an applicant's familiarity and comfort with technology. If someone cannot manage a Zoom or Webex interview, how effectively can they be expected to use a mobile device complete with accountability and reporting software? The transition to a more digital age arrives in time for the tech-savvy millennial generation, who won't think twice about remote processing.

Clients' expectations grow as the world becomes more complex and risks—both old and new—are added to the list of security officer tasks and concerns. Finding people who will be alert, attentive, pleasant, and professional in appearance has historically been the source of success for private security human resources staffing specialists. Their tasks are aided by technological advances, but complicated by generational tendencies and public health roadblocks.

"We are living through arguably the most accelerated amalgamation of technology and public health concepts in human history," says Dobrin. One thing will always be for certain though: human resources staff must function in a constant state of urgency and innovation, given that the phone rarely stops ringing and the operations department's "needs lists" will always be in the email inbox early each morning.

CHRIS STUART IS VICE PRESIDENT OF TOP GUARD SECURITY. EMPLOYED IN THE SECURITY INDUSTRY SINCE 1988, HE HAS SERVED ON SEVERAL ASIS COUNCILS AND THE COMMONWEALTH OF VIRGINIA'S PRIVATE SECURITY SERVICES ADVISORY BOARD. HE IS PAST PRESIDENT OF THE VIRGINIA SECURITY ASSOCIATION.

George Barlow Brown
IT Manager, Real-Time Crime Center
City of New Orleans

©2020 Genetec Inc. Genetec and the Genetec logo are trademarks of Genetec Inc., and may be registered or pending registration in several jurisdictions.

Everyday force multiplier.

"We can be where public safety agencies can't be, and give them video when they need it most."

Making New Orleans safer for citizens, businesses and visitors matters. Genetec solutions have helped the city's crime center give public safety agencies greater situational awareness — saving them 6,000 hours of investigation time last year.

genetec.com/everyday

Protect the everyday.

Genetec™

For product info #26 securitymgmt.hotims.com

GSX+ PRODUCT SHOWCASE 2020

Take the GSX+ Product Showcase with you anywhere—check it out online any time at **asisonline.org/2020GSXProductShowcase**

CREDENTIAL MANAGEMENT

AMAG Technology

www.amag.com

#303

AMAG Technology announced Symmetry Mobile, a Web credential application designed for AMAG's Symmetry Bluetooth readers. Symmetry Mobile supports COVID-19 and return-to-work guidelines, allowing for social distancing and a frictionless setup. This credential management platform offers a solution for organizations relying on mobile devices to access secured doors, eliminating the need to physically interact with security personnel or visit a badging office. The Mobile Credential Portal allows for remote central management of credentials, photos, and devices. The app and the reader integrate with Symmetry Access Control and other access control systems, and the platform supports multifactor authentication when used with a PIN or biometric marker on Android and Apple iOS devices.

ACCESS CONTROL

Continental Access

www.cicaccess.com

#304

The new CA4K Access Manager app, now available in the iTunes and Google Play stores, adds another level of mobile control to CA4K Enterprise Integrated Access Control Software developed by **Continental Access,** a Napco Security Group Company. The app—which also supports push notifications or emails in an emergency, threat level escalation, or lockdown events—acts as a virtual enterprise workstation on any smart device, allowing for management of threat levels, lockdown, status, and personnel. It also provides control of up to 32,000 doors, wireless PIN/Prox locks, elevators, and entryways, including their global or APB-area lock down.

ACCESS BOLLARDS

Pedestal PRO
www.pedestalpro.com
#305

Pedestal PRO's customizable pedestal solutions offer a choice of flush or surface-mount devices to improve freestanding access control bollards along your perimeter. Here, Comelit's 3454HD is mounted next to ProdataKey's Touch IO reader for a sleek, brushed stainless steel design. All fasteners are tucked away, hidden by an internal base plate accessible through a back panel. One of many customizable models, all bollards feature premium architectural aesthetics that can appeal to architects, engineers, business owners, and users. Standard models ship within 24 hours; custom orders require between 12 and 15 business days.

SIGNAL DETECTION

Research Electronics Inc.
www.reiusa.net
#306

REI (Research Electronics Incorporated) developed a portable spectrum analyzer that assesses radio frequency (RF) energy in a variety of environments. The new Mobility Enhanced Spectrum Analyzer (MESA) is a handheld RF receiver that detects known, unknown, illegal, disruptive, or interfering transmissions across a wide range of frequencies, up to 12 GHz when used with the Down Converter antenna. The MESA includes testing modes for RF spectrum analysis, Wi-Fi, Bluetooth, mobile bands, and a new mode that displays like a broadband receiver. With a polycarbonate body only slightly larger and heavier than a DSLR camera, MESA is also the only solution of its kind to be completely touch-screen controlled.

GUARD BOOTHS

B.I.G.
www.bigbooth.com
#307

B.I.G. prefabricated guard shacks offer a way to reduce installation times and expenses by meeting the energy and building codes of every U.S. state. Along with reducing operating costs and stretching design budgets, B.I.G. also offers bullet resistant construction with non-exposed armor plate.

SYSTEM ON A CHIP

Hanwha Techwin
ww2.hanwhasecurity.com
#308

In every market and for every application, the need for intelligent networked surveillance solutions remains. **Hanwha Techwin's** new product development is the Wisenet 7 System on a Chip (SoC). Developed in-house and built in Korea, new features and analytics for Wisenet 7 continue to come online, with it becoming the company's most technology-intensive, innovative, and feature-rich SoC.

VISITOR SCREENING

Allied Universal
www.aus.com
#309

Allied Universal enhanced its advanced artificial intelligence HELIAUS technology platform to include a new visitor screening application, helping keep facilities and employees secure during the COVID-19 pandemic. The visitor screening application includes new suggestions for workflows that can help with visitor screening, social distancing management, workplace signage, and maintaining a safe and clean workplace. The information electronically collected by HELIAUS during screening or custom workflows is fed into the platform's artificial intelligence engine, which recommends improvements to the facility's condition.

SPEAKERS

AXIS Communications
www.axis.com
#310

AXIS's C1410 Network Mini Speaker is a PoE powered standalone unit that can be placed on walls or ceilings to enhance existing security systems in small, indoor spaces and tight corridors. The speaker's small, flexible design features easy integration with any network video, access control systems, and Voice over IP (VoIP). With a built-in PIR sensor, audio messages can be delivered in response to detected motion. The speaker's built-in memory supports prerecorded messages and live security notifications. A built-in microphone allows for remote health testing so end users can confirm that the system is always working.

ORGANIZATIONAL FLEXIBILITY

TEAM Software
www.teamsoftware.com
#311

With **TEAM Software's** holistic, all-in-one software, clients can adjust operating procedures, workflows, and reporting requirements in response to compliance requirements from government entities—while remaining accountable to an organization's customers, contracts, employees, and leadership. When implemented and leveraged correctly, a holistic software solution tailored to a client's industry can keep business operations stable and compliant in the face of change, allowing for flexibility whether from the back office or the field.

LIABILITY INSURANCE

Brownyard Group
www.brownyard.com
#312

More than 70 years ago, **Brownyard Group** pioneered the development of liability insurance coverage specifically for the security guard industry with its Brownguard program. One of the largest U.S. insurance providers, the company works through an admitted insurer for the security guard, private investigative, and alarm industries. Brownyard Claims Management, Inc. (BCM) is a loss-prevention and full-service claims facility, offering claim settlement services, fully automated systems, and technology solutions.

SECURITY SOLUTIONS

G4S
www.g4s.com
#313

Through a risk-based approach, **G4S** offers a customized, multilayered security program that allows clients to stay focused on their business initiatives. With a combination of security professionals, methods, and technology, G4S designs integrated security solutions to manage risk, drive compliance, and provide business value. The company also offers a range of capabilities, including risk consulting and intelligence services, systems integration and monitoring, AMAG Technology software solutions, and security professionals to protect people, property, and other assets.

MAIL SCANNER

RaySecur
www.raysecur.com
#314

Offering a quick setup, MailSecur from **RaySecur** can detect more and smaller threats than x-ray mail scanners—useful as companies receive thousands of mail-borne threats every year. MailSecur can be up and running in just 30 minutes and requires no special certification or screening to operate. This solution is the first mail scanner designated by the U.S. Department of Homeland Security as a Qualified Anti-Terrorism Technology and is being used by the security teams of major companies and world leaders.

METAL DETECTORS

Garrett Metal Detectors
www.garrett.com
#315

Garrett's Quick-Q technology offers quick access into stadiums, arenas, outdoor events, convention centers, and concert halls. This technology can move high volumes of patrons through events, reducing line queues and large crowds outside the venue. When used with Garrett's walk-through metal detector, the PD 6500i, fans do not need to divest themselves of their cell phones or other small metallic items to be screened, improving throughput rates of event attendees.

ALARM LOCKS

Alarm Lock
www.alarmlock.com
#316

Alarm Lock, a division of Napco Security Technologies, presents Trilogy Networx Wireless Access Locks, now certified with Lenel Version 7.6 OnGuard Integrated Access Control and Video Security Platform. They feature a digital keypad and/or built-in smart reader, plus the longest battery life and field-proven low-maintenance. Networx Wireless Access Control Solutions can replace standard locks on any door in under an hour, with no wires to run and no access panels or power supplies to buy or in-stall. The locks provide an access system with advanced functions, including automatic schedules, event logs, and support for 2,000 doors and 5,000 existing identification cards or badges.

CEIA USA • THREAT DETECTION THROUGH ELECTROMAGNETICS

PMD2
Plus Elliptic

WHEN THE SMALL STUFF IS A BIG DEAL, CHOOSE CEIA.

Feel confident and secure without slowing anything down.

With over 50 years of experience in designing and manufacturing metal detectors, CEIA set the standard for high-volume security screening, keeping the lines moving and the crowds secure. Our walk-through metal detectors can detect even the smallest metallic objects while still providing optimal immunity to environmental interference.

HI-PE
Plus

FEATURES:

- Superior detection and throughput
- Exceptionally high discrimination of non-threat items
- Compliant with the strictest security standards
- Unmatched reliability

WWW.CEIA-USA.COM

security@ceia-usa.com
833-224-2342

CERTIFIED SAFETY ACT

For product info #27 securitymgmt.hotims.com

GSX+ PRODUCT SHOWCASE

OCCUPANCY CONTROL

Hanwha Techwin
ww2.hanwhasecurity.com
#317

Hanwha Techwin's full suite of health and safety intelligent solutions can readily adapt to the requirements of any changing business environment. Its Occupancy Monitoring System combines 4K camera resolution with edge-based AI video analytics, allowing clients to easily maintain safe building occupancy levels to protect employees and customers. The application provides retailers, houses of worship, museums, entertainment facilities, restaurants, and more with highly accurate, real-time data on the number of people in a facility at any given time.

SECURITY OFFICERS

PalAmerican Security
www.palamerican.com
#318

PalAmerican Security employs a 12-step selection process when considering applicants for its professional security officer program. Those qualified and accepted individuals are then provided with professional, vertical-specific training, and additional on-site training designed to exceed industry standards throughout North America. PalAmerican professional security officers focus on customer service and are backed by industry-leading security training.

WEAPONS DETECTOR

CEIA Metal Detectors
www.ceia-fmd.com
#319

CEIA's MSDi High-Performance Ferromagnetic Weapons Detector is specifically designed for easy integration of ferromagnetic weapons detection in covert access control. The MSDi's small footprint allows for the concealment of ferromagnetic detection technology inside ornamental structures and combines the features of MSD and MSD EVO in a single, compact device. Extremely durable and reliable, MSDi offers high and uniform sensitivity with detection over a person's entire height.

SECURITY SOLUTIONS

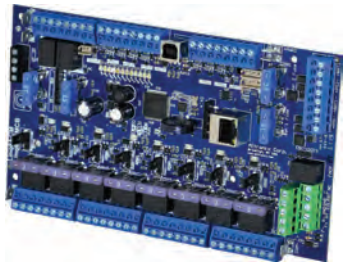
SECURAMERICA

SecurAmerica
www.securamerica.com
#320

SecurAmerica offers innovative contract security service solutions across the United States, with a business model based on creating and delivering operational excellence to customers by selecting the right people, training them to exceed clients' requirements, and providing them with a culture that is focused on 100 percent customer and employee satisfaction. SecurAmerica strives to deliver value, cost effectiveness, and results to all customers.

POWER CONTROLLER

Altronix
www.altronix.com
#321



Altronix introduced the LINQ8ACM Dual-Voltage Access Power Controller with LINQ Network Power Management. This new solution facilitates a wide range of locking devices while providing network monitoring, reporting, and control of eight independently controlled fuse or PTC protected access control outputs. For quick on-site verification, the LINQ8ACM is equipped with bi-color LEDs which indicate 12 or 24VDC on each of the eight outputs. The LINQ8ACM Dual-Voltage Access Power Controller is manufactured in the United States and backed by a lifetime warranty.

MISSION AWARENESS AND REVIEW

Esri
go.esri.com
#322

Esri's ArcGIS Mission is a command and control system that organizations—from disaster response and law enforcement agencies to executive protection and event security teams—can use to streamline mission management, gain situational awareness during active missions, provide geospatial-based peer-to-peer communication in the field, and conduct post-mission reviews. ArcGIS Mission offers the core capabilities of other tactical situational awareness solutions, but it also streamlines mission workflows and integrates directly with existing security technologies to provide new capabilities.

IDENTIFY THE THREAT BEFORE IT SURFACES

MZ 6100
MULTI-ZONE
DETECTION

MZ 6100 Walk-Through Metal Detector

With the rise of security threats, put your trust in an American-made product that you can rely on to keep your patrons safe.

GARRETT®
METAL DETECTORS

MADE IN THE USA

Email: security@garrett.com
Toll Free (U.S. and Canada) **800.234.6151**
Tel: **1.972.494.6151**

ISO 9001 CERTIFIED

For product info #28 securitymgmt.hotims.com

FIRE ALARMS

StarLink
www.starLinkLTE.com
#323

Instead of installing a new fire alarm, users can update communications to LTE Cellular to replace vanishing, costly copper POTS lines, or old sun-setting 3G/CDMA radios. Universal StarLink Fire Dual Path Communicators are an easy-to-deploy, low-cost solution that ensure any brand 12V/24V FACP keeps communicating quickly to first responders through AT&T and Verizon LTE networks. NFPA and UL fire code compliant and requiring no extra power supply or conduit, **Napco Security Technologies'** StarLink Fire Communicators can be quickly installed and replace two POTS lines per fire panel.

SECURITY SERVICES

Special Response Corporation
www.specialresponse.com
#324

For more than 30 years, **Special Response Corporation** has provided security, becoming a national leader for its protection of both personnel and property, providing security consulting and services to protect business and industry in homeland security threats, natural disasters, and manmade disasters. Past assignments include executive protection, plant downsizing or closure, labor unrest, and civil disturbances. Special Response team members have backgrounds in law enforcement and/or the U.S. Armed Forces—personnel who have been professionally recruited, screened, and trained.

SPEAKER GUARDS

Safety Technology International
www.sti-usa.com
#325

Big or small, **STI** (Safety Technology International) has a wire guard to fit it all. New heavy-duty 9-gauge speaker guards are constructed with a corrosion-resistant polyester coating and are recommended for areas of severe abuse or where it is imperative that speakers continue to operate. Fast and easy to install, the cages protect speakers and other large devices against vandalism, theft, and damage. They are available in two sizes and guaranteed for three years against breakage in normal use. Several additional wire guard models and sizes are also available for smoke detectors, motion detectors, emergency lights, clocks, cameras, and more.

SECURITY FENCES

AMICO Security
www.amicosecurity.com
#326

AMICO Security's Chameleon Perimeter Security System allows users to upgrade an existing chain link fence to the AMIGUARD Perimeter System. By using the existing fence posts, Chameleon's High Security Curtain Wall system upgrades the existing fence to a perimeter system with anti-cut and anti-climb features, while the AMICLAMP design allows for the integration of the AMIGUARD Infini-Rail. The Chameleon system works with post sizes including 1-7/8", 2-3/8", 2-7/8", 4", and 6-5/8." It also comes in various finishes.

SECURITY BOOTHS

Par-Kut International
www.parkut.com
#327

Par-Kut International's Presidential Series security booth comes completely factory assembled and can serve as both an access control point and as a visitor information booth. Ideal for school grounds, the guard shelter design blends into the surrounding classic architecture of school buildings. Further, while in development of the project, Par-Kut and the architect can collaborate to ensure a structure well-suited to serve the application functionally and that provides long-term value. The welded steel Par-Kut guard building offers both comfort and durability.

OCCUPANCY MANAGEMENT

HID
www.hid.gl/rtls
#328

HID Location Services combines a hardware and software solution for delivering actionable occupancy data that scales based on the needs of the facility. Integration with third-party systems allows customers to understand building entry and exit; gauge building occupancy by floor or room; set up virtual security zones and automate alerts or alarms for violations; and locate building occupants in the event of an emergency. HID Location Services can be used as part of an organizational strategy for enabling a safe return-to-work now and create a safer, more secure, efficient, and optimized environment when it's business as usual.

COMMERCIAL SECURITY

ADT Commercial

Powered by Experience. Driven by Excellence.™

ADT Commercial
www.adt.com/commercial
#329

ADT Commercial, a provider of commercial security, fire, life safety, and risk consulting services, supports more than 300,000 customer locations with a network of more than 4,500 experts throughout 150 locations and two monitoring and operations centers. Built on a foundation of decades of customer service and industry expertise, ADT continues to expand its portfolio of solutions, geographic reach, and commercial field operations.

ANTI-LIGATURE LOCKSETS

Marks USA
www.marksusa.com
#330

New to the **Marks USA** LifeSaver Healthcare Series are the 195BH and 5BH D-Lig Slide Behavioral Health Locksets. These Grade 1 anti-ligature locksets are available in cylindrical or mortise, and they are BHMA156.34 Anti-Ligature Trim Standard compliant. The solid cast stainless steel 5-point ligature resistant slide slides down freely in the locked or unlocked position. The D-Lig Slide is also tamper-proof—bolted for durability and easy installation—and available with an antimicrobial finish option.

ALARM MANAGEMENT PLATFORM

Genetec
www.genetec.com
#331

Genetec Mission Control is a collaborative decision management system providing organizations with new levels of situational intelligence, visualization, and complete incident management capabilities. Mission Control empowers organizations to move beyond simple event and alarm management by collecting and qualifying data from thousands of sensors and security devices, spotting the most complex situations and incidents, and guiding security teams in their response following organization-specific processes and compliance requirements.

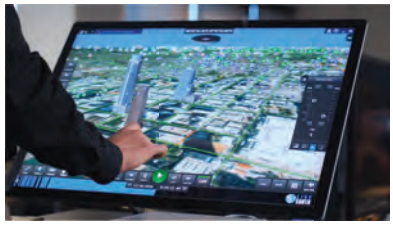
METAL DETECTOR

CEIA Metal Detectors
www.ceia.net
#332

CEIA's PMD2 Plus elliptic walk-through metal detector can detect a large range of threat objects composed of magnetic, nonmagnetic, and mixed alloys. The enhanced multi-zone metal detector can operate in high profile checkpoints and architecturally demanding environments. Twenty-two embedded security standards, discrimination technology on personal metal items, rapid transit flow, and extremely versatile visual and acoustic signaling capability are some of the main features offered by this model. Optional weather resistant protection is also available.

INCIDENT MANAGEMENT

Live Earth
www.liveearth.com
#333



Live Earth is an open platform, SaaS-based application, with roots in the U.S. Department of Defense. The platform leverages a technology stack that provides real-time situational awareness and an advanced approach to alerting and incident management. Live Earth, a geo-temporal data visualization technology, fuses millions of disparate data sources and presents them on a common operational picture. This enhanced visualization advances business operations globally with increased safety and security, business intelligence, and operational efficiency.

ACCESS CONTROL

Vanderbilt U.S.
www.vanderbiltindustries.com
#334

With something for everyone, **Vanderbilt U.S.** offers a fully integrated solutions portfolio that features Web-based, cloud-based, and on-premises access control solutions, as well as integrated or standalone video management platforms. Organizations of all sizes—from small-sized businesses to global enterprises—can use the suite of products presented by the Vanderbilt brand, which also offers dedicated customer service, product development, and training.

WHAT IS GSX+?

IT'S BEEN A LONG YEAR with new challenges faced and vital lessons learned along the way. Later this month, 21–25 September 2020, thousands of security professionals from around the globe will gather to share security best practices in a world reshaped by COVID-19. As a true sign of the times, they won't be gathering in person.

In lieu of the physical Global Security Exchange (GSX) event, ASIS International created Global Security Exchange Plus (GSX+)—a new virtual experience designed to deliver the world-class education, networking, and marketplace that security professionals around the world have come to expect from GSX.

Education

The GSX+ education program, built by security professionals for security professionals, offers attendees more than they could experience at any previous GSX. Sessions are being recorded and made available on-demand to All-Access attendees through the end of the year, making it possible to attend every session presented at GSX+. And the continuing professional education (CPE) credits you'll earn reflect that—attendees can earn up to 25 CPEs towards recertification.

GSX+ sessions will tackle the most pressing issues facing security professionals today, from insider threats in a borderless work environment to bridging the gap between cyber and physical security. Other topical sessions cover drones, artificial intelligence, and ESRM.

The education lineup, available at *GSX.org/sessions,* is divided into tracks to help you find the sessions most valuable to you. The tracks include:

- Digital Transformation and Information Security
- Leadership and Managing Organizations
- National Security
- Physical and Operational Security
- Risk Management

Networking

Daily networking events help keep the security community connected and offer a venue for discussing the newest trends, ideas, and opinions. The GSX+ platform allows users to opt-in to live networking throughout the entire week, with the ability to request one-on-one meetings with fellow attendees. Stay tuned throughout the week for additional opportunities to network with peers in one-on-one meetings, small group discussions, and larger networking events.

Marketplace

The core of any industry event is the ability to browse new technologies, watch demonstrations, meet potential partners, and learn about new solutions. All this is available in the GSX+ virtual Marketplace.

Attendees can browse the Marketplace and attend live scheduled product demos and tech talks from exhibiting companies or view them on-demand at attendees' convenience. GSX+ provides matchmaking between exhibitors and attendees to

help attendees find exactly the products and services they require. Beyond this, attendees can reach out to companies directly within the platform to request private one-on-one meetings or product demos to see technology in action and ask questions.

The Always-On Experience

As a virtual event, GSX+ will be accessible 24 hours a day, with live content recorded and available on-demand shortly after its airtime. When you are ready to learn, the content is ready for you to experience. It is also a cyber-safe event, with SSL/TLS encryption technology that is audited annually by third parties to ensure the safe transmission of data.

At a time when it is more important than ever to ensure that you bring maximum value to the table with your skills and knowledge, GSX+ delivers security professionals the tools they need to improve their security practice.

With opportunities to participate ranging from the All-Access Pass to the Marketplace-Only Pass, GSX+ is an experience not to be missed. Learn more at *GSX.org*.

BLOCKCHAIN: A GUIDE FOR SECURITY PROFESSIONALS

Blockchain is making major inroads in the security industry—in areas such as identity management, smart contracts, and video verification. Newly released ASIS Foundation research is designed to help security professionals better understand the technology, its security advantages, and its implications for security management.

Blockchain: A Guide for Security Professionals, the first report in the foundation's new Digital Transformation Series, provides a practical overview of the facets of blockchain that are most relevant to security practitioners. Learn more about how the technology is already being applied and the considerations to be aware of before implementation.

This study is based on 30 interviews with blockchain and cryptocurrency experts, a survey of more than 2,000 security professionals, and a literature review of more than 150 reports, studies, books, research papers, and more.

Key findings examined in the report include:

- Blockchain is a type of database, though a powerful one.
- Security professionals around the globe are generally unfamiliar with blockchain, and their companies are not using the technology.
- Blockchain offers many security advantages.
- Blockchain may be poised for mass adoption, but it's not quite there yet.

Visit *GSX.org* to learn more about sessions, speakers, and more.

ASIS GLOBAL BOARD OF DIRECTORS

PRESIDENT
- Godfried Hendriks, CPP
  Revolution Retail Systems
  Alkmaar, The Netherlands

PRESIDENT-ELECT
- John A. Petruzzi, Jr., CPP
  G4S Americas
  New York, New York, USA

SECRETARY/TREASURER
- Malcolm C. Smith, CPP
  Qatar Museums
  Doha, Qatar

CHIEF EXECUTIVE OFFICER
- Peter J. O'Neil, FASAE, CAE
  ASIS International
  Alexandria, Virginia, USA

AT-LARGE DIRECTORS
- Pablo Colombres, CPP
  GIF International
  São Paulo, Brazil
- Timothy M. McCreight, CPP
  The City of Calgary
  Calgary, Alberta, Canada
- Darren T. Nielsen, CPP, PCI, PSP
  Guidehouse
  Peoria, Arizona, USA
- Jaime P. Owens, CPP
  Panama Canal Authority
  Panama City, Panama
- Malcolm B. Reid, CPP
  Brison
  Richmond, Virginia, USA
- Ann Y. Trinca, CPP, PCI, PSP
  SecTek
  Tysons, Virginia, USA

EX-OFFICIO VOTING
- Cy A. Oatridge, CPP
  OSG
  Tacoma, Washington, USA
- Joe M. Olivarez, Jr.
  Jacobs
  Houston, Texas, USA

EX-OFFICIO NON-VOTING
- Bernard D. Greenawalt, CPP
  Retired
  Tinley Park, Illinois, USA
- William D. Moisant, CPP, PSP
  Retired
  Murrells Inlet, South Carolina, USA

- Blockchain shouldn't be a technology seeking an application.
- When blockchain is a good solution, any one of four different types of blockchain might be the best choice.
- Blockchain must confront various security issues and other challenges.
- Trust is the key philosophical issue.
- Successful blockchain use cases have yet to transform into lasting implementations.

The complimentary executive summary is available at *asisfoundation.org*. ASIS members can download the full report—a $125 value—for free.

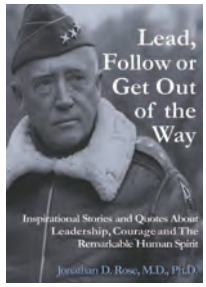
The next topic to be addressed in the ASIS Foundation Digital Transformation Series is artificial intelligence, to be published early in 2021.

MEMBER BOOK REVIEW

Lead, Follow or Get Out of the Way: Inspirational Stories and Quotes About Leadership, Courage, and the Remarkable Human Spirit. **By Jonathan Rose, CPP, PCI, PSP.** AuthorVista LLC; available from Amazon.com; 160 pages; $12.99.

It is said that war brings out both the best and worst in people. Using narratives from wars and other instances of upheaval, author Jonathan Rose, CPP, PCI, PSP, looks to some well-known and more obscure historical figures for leadership insights and inspiration in *Lead, Follow or Get Out of the Way.*

Most of the figures introduced have military credentials, whether the leadership skills under examination are those of Julius Caesar, Joan of Arc, or 12-year-old Seaman Calvin Graham. Graham served in the U.S. Navy in late 1942 and—in three short months—he was awarded the Bronze Star, the Purple Heart, and a Navy Unit Commendation before being arrested and discharged two days before his 13th birthday. While Graham undoubtedly is an inspiration, one can argue that Caesar, whose leadership skills were impressive, was also responsible for the deaths of millions of people and the end of democracy in ancient Rome. Regardless of your opinion of Caesar, there are reasons he is still studied some 2,000 years after his death.



This book consists of 11 chapters, each focusing on one positive character trait: courage, perseverance, faith, friendship, hope, duty, dedication, wisdom, honesty, determination, and victory. Each inspirational story is followed by related quotes from numerous individuals based on that chapter's theme. Each story takes just a few minutes

to read. The quotes that follow come from three sources: individuals from the arts, science, politics, sports, and business; anonymous contributors; and the author.

While this is not a security book per se, its focus on leadership is directly related to the management of the security function. Leadership is the key element that, along with training and communications, can bring out the best or the worst in people. While the book is short enough to read in a single sit-down, it is also filled with many observations and facts that give pause for thought long after, as well as reason to return to the book again and again.

REVIEWER: *Glen Kitteringham, CPP, has worked in the security industry since 1990. He is president of Kitteringham Security Group Inc., consulting with companies around the globe, and teaches security and emergency management courses at the University of Calgary and the Justice Institute of British Columbia.*

ASIS WEBINARS

SEPTEMBER

3 Closing the Last Physical Security Gap

10 How Radar Technology Can Help Better Secure Your Perimeter

ASIS GLOBAL EVENTS

SEPTEMBER

21–25 Global Security Exchange Plus (GSX+)

ASIS ONLINE LEARNING

OCTOBER

6 CPP Virtual Study Group

7 PSP Virtual Study Group

8 APP Virtual Study Group

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

CERTIFICATION PROFILE

KEVIN DOSS, CPP, PSP

"Security chooses you." Early in his career, Kevin Doss wanted to be a state trooper or secret service agent. "But life had other plans for me," he says.

While serving in conservation law enforcement, Doss experienced a call to protect others. He transitioned to a role in security—first as a project manager for a financial institution and then for a major security integrator. His career developed there, as he earned a promotion and began working as a consultant on the integration side of security.

His ascent through the security ranks is marked by a firm devotion to constant self-improvement—which benefits the people his policies are designed to protect.

"In matters involving security, if you are not moving forward, you are falling behind," he says. "Security is something bigger than self—a greater good. This fact cannot be overstated, as it drives the security professional to excel in making the world a safe place for all."

And as Doss sought to improve his security practice, he found that ASIS International certifications provided a great way to learn while improving his career standing.

"Organizations seek competent professionals," Doss explains. "ASIS board certifications provide prospective employers with the leading industry credentials to demonstrate an individual's proficiency and commitment to their profession."

He joined ASIS and the Central Pennsylvania Chapter in 2002. Under the mentorship of Milton "Mick" Moritz, CPP, he decided to pursue the Physical Security Professional (PSP®) designation—and successfully passed the exam in 2003.

"Once immersed in the certification process, I realized that the real value of the program was not just the certificate, but rather the knowledge that it bestows," he reflects. "It identified gaps in my security knowledge—that I didn't actually know what I thought I knew. When my employers saw the results of my certification efforts and the relationships that I built within ASIS, they asked the entire division to join and offered to pay for their certifications as well."

The certification process kicked off a lifelong pursuit of professional development. Doss earned the Certified Protection Professional (CPP®) certification in 2005 and completed the Master's of Security and Risk Management degree at the University of Leicester (United Kingdom) in 2009, the same year he founded his own security consulting firm—Level 4 Security, LLC.

As his career has continued to develop, Doss has sought to pave the way for security professionals following in his footsteps. Since 2008, he has served ASIS as the PSP Board Certification Review Program Advisor and lead instructor for both the online and in-person classroom programs.

He helped develop the PSP Virtual Study Group sessions that will begin in October 2020, and Doss will serve as the discussion moderator for that group of aspirants looking to earn their own PSP certification.

"ASIS board certification can open doors and differentiate you from other applicants and may increase your earning potential, but most of all, it can help you to become a better professional," he says.

"Helping other security professionals achieve certification is a tremendous opportunity and responsibility for me. It is one way I give back to ASIS International."

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

JUDICIAL DECISIONS

DISCRIMINATION. The U.S. Supreme Court found that the Civil Rights Act of 1964 protects gay and transgender employees from sexual orientation discrimination.

The 6–3 decision officially expands protections to the LGBTQ community, prohibiting employers from discriminating against a person's sexual orientation or gender identity.

"An employer who fires an individual for being homosexual or transgender fires that person for traits or actions it would not have questioned in members of a different sex. Sex plays a necessary and undisguisable role in the decision," wrote Associate Justice Neil Gorsuch in the majority opinion. "An individual's homosexuality or transgender status is not relevant to employment decisions. That's because it is impossible to discriminate against a person for being homosexual or transgender without discriminating against that individual based on sex."

The decision will allow people who believe they have been discriminated against in the workplace because of their sexual orientation or gender identity to file lawsuits.

Prior to the formal ruling, more than half of U.S. states gave no such protections for employees. (*Bostock v. Clayton County, Georgia*, Supreme Court of the United States, No. 17-1618, 2020)

DISASTER RELIEF. Xavier University of Louisiana agreed to pay $12 million to settle charges that it submitted false claims of damages caused by Hurricane Katrina to U.S. relief programs.

Xavier University—which also agreed to cooperate with a U.S. Department of Justice (DOJ) investigation into other parties involved—was accused of using an architecture and engineering firm to improperly access U.S. federal relief funds for its facilities, including the gymnasium, student center, and electrical grid, according to the DOJ.

The school allegedly exceeded the amount it should have received as part of the rules of the Federal Emergency Management Agency 's (FEMA's) Public Assistance (PA) program. The Robert T. Stafford Disaster Relief and Emergency Assistance Act gives FEMA the power to approve PA program funds to schools and universities, allowing the institutions to restore their facilities to a pre-disaster condition.

A whistleblower filed a lawsuit alleging that the university's architecture firm, AECOM, submitted false and misleading claims on behalf of other applicants seeking funds to repair or replace facilities damaged by the 2005 Category 5 storm. From 2005 through 2019, AECOM received more than $300 million from the PA program while working as a technical assistance contractor for the university, responsible for site evaluations and preparing repair estimates.

AECOM is also accused of inflating estimates, providing FEMA with inaccurate information on facilities' pre-disaster status, and using other false information to increase the funds its clients were awarded from the PA program. The lawsuit claims that certain applicants were jointly liable for these exaggerated estimates, signing off on or supporting the AECOM reports. (*United States ex rel. Robert Romero v. AECOM, Inc., et al.*, U.S. District Court for the Eastern District of Louisiana, No. 16-cv-15092, 2020)

PHOTOS BY iSTOCK

LEGAL HIGHLIGHTS

COURT CASES

ISSUE: Murder
CASE: *United States v. Carrillo*
VENUE: U.S. Dist. Ct. N. Dist. of California
STATUS: Charges filed
SIGNIFICANCE: Steven Carillo was charged with murder and attempted murder for a shooting that killed a Federal Protective Service officer and injured another security officer.

ISSUE: Discrimination
CASE: *United States v. Bel USA LLC*
VENUE: U.S. Dist. Ct. S. Dist. of Florida
STATUS: Settled
SIGNIFICANCE: The $100,000 civil penalty settled claims of discriminating against work-authorized non-U.S. citizens.

LEGISLATION

The Philippines

TERRORISM. Filipino President Rodrigo Duterte signed legislation into law that allows terror suspects to be held without charges or arrested without a warrant for a longer term.

The Anti-Terrorism Act of 2020 allows terror suspects in the Philippines to be held without charges or arrested without a warrant for up to 24 days. The country's constitution currently limits detention without specific charges to three days. The legislation also removes an existing fine—up to 500,000 pesos ($10,000 USD) per day of detention—for wrongfully holding a suspected terrorist.

Additionally, the law created a new Anti-Terrorism Council, which has the ability to designate individuals or groups as suspected terrorists and place them under surveillance or arrest. Anyone accused of involvement in a terrorist attack could receive a prison sentence of life without parole. Any individual found to have joined a designated terrorist group could be sentenced to up to 12 years in prison.

Opponents of the law, including nationalist groups, religious officials, media watchdogs, and human rights organizations, claim it could be used against the administration's critics, especially given the act's broad definition of terrorism. One of the bill's definitions of the crime of terrorism is "acts intended to cause extensive damage or destruction to a government or public facility, public place, or private property."

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

United Kingdom

CORONAVIRUS. The United Kingdom instituted new rules for anyone entering its borders, ordering all arrivals to self-isolate for 14 days—the length of time it takes for symptoms of the COVID-19 virus to appear.

Whether tourist or citizen, everyone arriving in the Channel Islands, England, Ireland, the Isle of Man, Scotland, or Wales must provide an address where he or she will be self-isolating for the duration of the two-week period. Anyone found violating the self-isolation rule could be fined up to £1,000 ($1,300 USD), while those failing to provide an accurate address for the site of their isolation could be fined up to £3,200 ($4,200 USD).

If no symptoms of the virus have appeared after the two weeks, the person can stop self-isolating. If symptoms do appear, the government is asking persons to remain in self-isolation—extending the restriction to all others living in the same household.

Some persons are exempt from the new rules, such as those traveling from within Ireland, the Isle of Man, and the Channel Islands to other parts of the United Kingdom; defense personnel; and diplomats, representatives of international organizations, representatives at an international or UK conference with certain privileges and immunities, and their families or dependents.

INTERNATIONAL LEGISLATION

Lebanon

Corruption. Lebanese legislators adopted an anti-corruption law, removing established banking secrecy rules.

Under the new law, special investigators can access the bank accounts of current and former state officials—including cabinet ministers, lawmakers, and civil servants. Any investigations must be limited to the Special Investigation Commission and the National Anti-Corruption Authority, according to Lebanon's state news outlet, National News Agency.

A Brookings Institution analysis found that, for 100 days in 2019, Lebanese protesters railed against corruption and called for the expulsion of everyone from ministerial posts because of widespread corruption.

The law, which was in development for eight years, was finally pushed to completion by the country's new government.

ISSUE: Retaliation
CASE: *EEOC v. Brookdale Senior Living Communities, Inc*
VENUE: U.S. Dist. Ct. E. Dist. of California
STATUS: Settled
SIGNIFICANCE: Brookdale agreed to an $80,000 settlement and other relief for firing an African American caregiver who complained about other employees' use of racially charged language.

ISSUE: Discrimination
CASE: *EEOC v. Albertsons Companies, Inc., et al.*
VENUE: U.S. Dist. Ct. S. Dist. of California
STATUS: Settled
SIGNIFICANCE: Albertsons paid a $210,000 settlement over a class national origin discrimination lawsuit that alleged a store manager harassed Hispanic employees for speaking Spanish.

China

FRAUD. The China Securities Regulatory Commission fined one of the country's largest pharmaceutical companies for a $4.3 billion accounting scandal, ordering the company to pay roughly ¥600,000 ($86,000 USD).

Falsified documents were used to transfer company funds that were used to trade in the company's own stock.

In late 2018 Kangmei Pharmaceutical Co. came under scrutiny for fraudulent financial reporting. A 2019 investigation revealed that fake bank deposits inflated the company's cash reserves, while falsified documents were used to transfer company funds that were used to trade in the company's own stock. The fraud ran from 2016 to 2018 and resulted in overstating the company's cash position by ¥29.9 billion ($4 billion USD).

The commission also blacklisted six Kangmei Pharmaceutical Co. executives, banning them from participating in the securities market and from working as executives or board members for at least 10 years. Another 22 Kangmei employees were fined a total of ¥5.95 million ($850,000 USD) in 2019 for their involvement in the fraud.

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

ELSEWHERE IN THE COURTS

FRAUD

A former U.S. Drug Enforcement Administration (DEA) employee pled guilty to charges of defrauding companies by posing as a CIA officer working on intelligence gathering. Garrison Kenneth Courtney, who conned $4.4 million out of roughly 12 companies, faces a maximum sentence of 20 years in prison. He told the companies to hire him and pay him a salary as a cover for his CIA operation; he also said that the businesses would be compensated through U.S. government contracts. (*United States v. Courtney,* U.S. District Court for the Eastern District of Virginia, No. 1:20-cr-00084, 2020)

DISCRIMINATION

The Union Pacific Railroad Company agreed to a $260,000 settlement to close a disability discrimination case brought by the U.S. Equal Employment Opportunity Commission (EEOC). The EEOC said that Union Pacific discriminated against a former employee, who once had a brain tumor, by not providing an individual assessment to determine if he could perform in his current position at a transportation center in Chicago, Illinois. Union Pacific agreed to the settlement but denied the allegations of discrimination. Along with the monetary fine, which will go to the former employee, the company will also train the Chicago service unit employees on protections provided by the Americans with Disabilities Act and will report all future disability discrimination complaints and denials of return to work (after a medical absence) requests to the EEOC. (*U.S. Equal Employment Opportunity Commission v. Union Pacific Railroad Co.*, U.S. District Court for the Northern District of Illinois, No. 19-cv-6021, 2020)

ESPIONAGE

Henry Kyle Frese, a former counterterrorism analyst for the U.S. Defense Intelligence Agency, was sentenced to 30 months in prison for repeatedly leaking classified information to two journalists. Prosecutors asked the court for a prison term of nine years for Frese's violations of the Espionage Act. The classified information Frese provided included revelations from several intelligence reports. Frese also conducted searches on classified government systems on behalf of the reporters and orally transmitted information to one of the journalists at least 12 times, according to the U.S. Department of Justice. (*United States v. Frese,* U.S. District Court for the Eastern District of Virginia, No. 1:19-cr-00304-LMB, 2020)

LEGAL HIGHLIGHTS

LEGISLATION

ISSUE: Police misconduct
BILL: S. 3912
VENUE: U.S. Senate
STATUS: Introduced
SIGNIFICANCE: Proposes a national registry tracking police misconduct and lowering legal standards to pursue criminal and civil penalties for police misconduct.

ISSUE: Corruption
BILL: Revision of Malaysian Anti-Corruption Commission Act 2009
VENUE: Malaysia
STATUS: Enacted
SIGNIFICANCE: Commercial organizations are liable if their employees or associates are involved in corrupt actions.

PHOTO COURTESY OF INTERFACE SECURITY SYSTEMS

VIDEO SECURITY SOLUTION

A strategic partnership between Interface Security Systems and OpenEye will allow enterprises to leverage the power of a 24/7 virtual monitoring system and access and management of video through a cloud-managed solution. Interface, a managed services provider delivering multiple surveillance and intelligence solutions, also offers retail, restaurant, and hospitality customers an interactive video monitoring solution. OpenEye's Web services platform includes cloud-managed solutions for enterprises seeking video security, business intelligence, and loss prevention systems. The partnership now offers clients advanced video and audio monitoring by life safety experts, real-time intelligence, streamlined investigation capabilities, advanced mobile features, and easy-to-use video management.

MERGERS & MOVES

Allied Universal ⇆ Phoenix Systems & Service, Inc.

The acquisition will expand Allied's technology services division in Illinois and throughout the United States.

STANLEY Security ⇆ Evolv Technology

STANLEY's investment in Evolv expands its portfolio, with security screening of concealed weapons that relies on artificial intelligence and allows for social distancing.

Trustworthy Accountability Group ⇆ JICWEBS

The two anti-fraud and brand safety organizations agreed to a merger that will extend to Europe, the United Kingdom, and the United States.

GlobalSCAPE, Inc ⇆ HelpSystems, LLC

The merged companies will focus on providing security and automation solutions to customers all over the world.

AWARD

Leica Geosystems was awarded the Security Industry Association's 2020 Best New Product Award for its Leica BLK247 at the virtual ISC West tradeshow. The real-time reality capture sensor monitors 3D environments with features that include thermal imaging.

CONTRACT

The Hawaii Department of Transportation selected NEC Corporation of America and Infrared Cameras Inc. to provide thermal temperature screening and facial recognition at the U.S. state's public airports.

ANNOUNCEMENTS

TRU-Vu Monitors offered a free guide on cleaning and disinfecting touch screens without damaging the screens, while Genetec made its digital evidence management system, Clearance, free to organizations in need of managing and distributing digital video evidence.

PARTNERSHIPS

EMERGENCY RESPONSE

AI weapons detection platform **ZeroEyes** partnered with emergency response data platform **RapidSOS** to enable sending of threat information directly to 911.

EMERGENCY ALERTS

BlackBerry Limited partnered with **Vodafone** to offer BlackBerry AtHoc, a real-time emergency alert and crisis communications solution.

VIDEO MANAGEMENT

Arcules partnered with **Milestone Systems** to deliver the Arcules-XProtect Hybrid VMS Solution, combining video surveillance as a service with video management software.

NEW PRODUCTS

Included in this month's solutions are a security platform, thermal cameras, and access control.

SURVEILLANCE MANAGEMENT | #901

Genetec Inc. released a new version of Security Center, the company's open-architecture platform that unifies video surveillance, access control, automatic license place recognition, communications, and analytics. The latest version offers stronger protection against video tampering and unauthorized export. It also helps administrators maintain their system more efficiently and reinforces the unification of communications with security systems. Video watermarking can also be enforced on all live feeds and footage exported from Security Center.

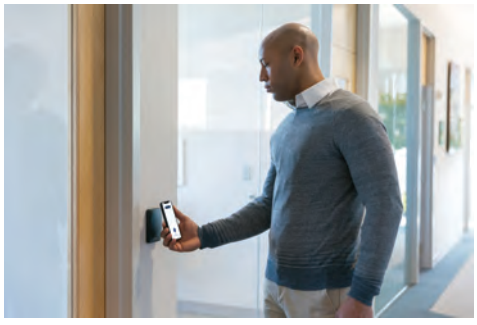
genetec.com

THERMAL CAMERAS | #902

Platinum CCTV released a new thermal body temperature sensing security camera, designed to help protect against the spread of disease by rapidly prescreening individuals before they enter a facility. The PT-BF5421-T Thermal/Visible Hybrid IP Security Camera provides accurate body temperature readings of plus/minus 0.3 degrees Celsius, while alerting staff to apply protocols when needed. Each thermal image is clearly seen, with both visible and audible alerts sent whenever a high body temperature is detected.

platinumcctv.com

FACILITY CONTROL | #903



LenelS2 announced its portfolio of solutions, part of Carrier Global Corporation's Healthy Buildings Program, designed to help protect people and assets and optimize building health and efficiency. Touchless access is possible with implementation of BlueDiamond mobile credentialing technology. Occupancy management and enhanced access control leverage data and control building access, such as providing access reports to support contact tracing. Proactive screening through access control solutions enables employees and visitors to self-assess their health and wellness via Web- and email-based tools prior to entering a building. LenelS2 offers three different solutions packages: Core, Enhance, and Elite.

LenelS2.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 #
14	Allied Universal	33
18	ADT Commercial	41
10	Altronix	25
100	AMAG Technology/G4S	02
06	Amico	13
03	Axis Communications	06
05	B.I.G Enterprises	10
23	Brownyard Group	58
27	CEIA USA	67
25	CEIA USA Ferromagnetic	61
12	esri	28-29
07	G4S	15
28	Garret Metal Detectors	69
26	Genetec	63
01	Hanwha Techwin America	2-3
04	HID Global	08
19	Live Earth	45
103	Magos Systems	07
16	Mission 500	39
31	Napco/Continental Access	86
105	Napco/Networx	12
24	PalAmerican Security	59
13	Par-Kut International	32
30	Raysecur	85
104	Raysecur	11
08	Research Electronics International	20
21	Safetey Technology International	51
02	SecurAmerica, LLC	4-5
09	Special Response	24
17	Team Software	40
102	Team Software	05
22	Zbeta Consulting	55

ADVERTISERS ONLINE

Allied Universal
www.aus.com

ADT Commercial
www.adtcommercial.com

Altronix
www.altronix.com

G4S
www.g4s.us

AMAG Technology/G4S
www.amag.com

Amico
www.amicosecurity.com

Axis Communications
www.axis.com

B.I.G Enterprises
www.bigbooth.com

Brownyard Group
www.brownyard.com

CEIA USA
www.ceia-usa.com

CEIA USA Ferromagnetic
www.ceia-fmd.com.

esri
www.goesri.com

Garret Metal Detectors
www.garrett.com

Genetec
www.genetec.com

Hanwha Techwin America
www.hanwhasecurity.com

HID Global
www.hidglobal.com

Live Earth
www.liveearth.com

Magos Systems
www.magosys.com

Mission 500
www.mission500.org

Napco/Continental Access
www.cicaccess.com

Napco/Networx
www.alarmlock.com

PalAmerican Security
www.palamerican.com

Par-kut International
www.parkut.com

Raysecur
www.raysecur.com

Research Electronics International
www.reiusa.net

Safety Technology International
www.sti-usa.com

SecurAmerica, LLC
www.securamericallc.com

Special Response
www.specialresponse.com

Team Software
www.teamsoftware.com

Zbeta Consulting
www.zbeta.com

**Security Technology supplement denoted in orange.*

SECURITY
MANAGEMENT

WHEREVER YOU ARE

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

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

MAGAZINE

Read the award-winning print publication from ASIS International.

APP

Download the digital magazine on iPad® or Android™.

WEB

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

SOCIAL

Join the discussion on Facebook and Twitter.

PODCAST

Hear what security professionals are talking about.

E-MAIL

Subscribe to the SM Daily and Weekly Newsletters.

FIVE RULES FOR CRISIS LEADERSHIP

MANY THOROUGHLY SAVVY EXECUTIVES FAIL TO TAKE THE POTENTIAL FOR CRISIS AS SERIOUSLY AS THEY SHOULD. THEY MIGHT HAVE GREAT SECURITY PLANS, OR THEY MIGHT BE FOLLOWING SO-CALLED BEST PRACTICES IN CRISIS MANAGEMENT, BUT THEY ARE STILL WOEFULLY UNDERPREPARED. **DR. JO ROBERTSON,** AUTHOR OF *EXECUTING CRISIS: A C-SUITE CRISIS LEADERSHIP SURVIVAL GUIDE,* SHARES HER TOP FIVE RULES FOR LEADING AN ORGANIZATION THROUGH TURBULENT TIMES.

1. **NO SUCCESSFUL CRISIS RESPONSE BEGINS ON THE DAY OF THE CRISIS.** It takes preparation to plan for crises and to proactively have the elements in place to suss out potential crises and derail them before they happen. This forward-thinking approach requires a structure and process not only for responding to a disruption and resuming operations quickly, but to stand a better chance of avoiding crises entirely.

   Ad hoc responses built on the belief that the organization has good people who know how to run things are not as effective as planning and practicing for success. What sports team would consider not practicing their best strategy for winning a championship? Just because they have top players doesn't mean those people will be adept at interacting with each other quickly when under pressure without practice.

2. **DO THE RIGHT THING.** Follow your mission statement. What are the things you explicitly state are core to your mission? If putting your employees or customers first is among them, then your leadership during a crisis must demonstrate that or it's just lip service.

   Truly leading in a crisis means making very hard decisions and leading by example.

3. **"TRUST US" NEVER WORKS.** In a crisis, you can't just spin the side of the story you want. You must provide information to the satisfaction of the key stakeholders you are trying to convince.

   Answer stakeholders' questions with specificity—this is key. For example, when communicating return-to-work decision making during the pandemic, successful organizations itemized circumstances that would either enable or stall reopening, such as a 14-day downward trajectory in COVID-related hospitalizations in states where the business operates.

4. **DON'T ASSUME YOU CAN MANAGE A CRISIS BY CONTINUING TO DO THINGS THE WAY YOU HAVE ALWAYS DONE THINGS.** There is huge value in understanding company culture, but, frankly, believing one knows what is the best practice when one has not experienced other contexts can create artificial blinders to potentially better ways of doing things.

5. **BREAK YOUR OWN NEWS.** Let's be clear: bad news doesn't smell sweeter with time. And it's certainly not going to go unnoticed the longer it's left to fester. Organizations that are up front about crisis response and mistakes will regain and retain customer trust faster than organizations that hope errors will go undiscovered.

© 2020 DR. JO ROBERTSON

HOW DO YOU KEEP YOUR PEOPLE SAFE FROM MAIL-BORNE THREATS?

MAILSECUR: THE NEW STANDARD IN MAIL SECURITY

Every year thousands of companies receive threats through the mail. While usually kept quiet, these have resulted in costly (and sometimes embarrassing) evacuations, injury, and even death.

MailSecur is the new standard in mail security. With its unique millimeter wave technology it can detect more and smaller threats than an X-ray mail scanner, is safe to use, and can be up and running in just 30 minutes.

And **MailSecur** has been designated by the US DHS as a Qualified Anti-Terrorism Technology, which provides you with important liability protections.

SECURITY MAILSECUR SCREENED

When your mail is stamped with the MailSecur stamp, your people know that you're looking out for them. And disgruntled employees know that it's not even worth sending a mail-borne threat because it will be detected.

Sign up to see a free, live demo of MailSecur and understand how well you can protect your people at **raysecur.com/sm-signup**

RAYSECUR™

THE NEW STANDARD IN MAIL SECURITY

www.raysecur.com | 617-855-9938 | info@raysecur.com

For product info #30 securitymgmt.hotims.com

MailSecur™ and **RaySecur**™ are trademarks of RaySecur, In

App: Virtual Enterprise Security Management Workstation in Your Pocket

Easy, Smart Management and Control of Doors, Lockdown, Threat Levels, Status, Control & Personnel

New! **CA4K® Access Manager App** adds another level of convenient intuitive mobile control to Continental Access' flagship CA4K Enterprise Integrated Access Control/Security/Video Management Software Platform, which also supports push notifications (or emails) in the event of an emergency, threat level escalation or lockdown events (shown). Built-in Mobile Credential - Ideal for schools, hospitals, multi-tenant & commercial buildings.

- **Supports any Smart Device** (smart phones, tablets); Available on iTunes® or Google Play®
- **Comprehensive Control of All Doors (1-32,000),** wireless PIN/Prox locks, readers, elevators & entryways
- **Activate & Control Global or APB Area-Specific Lock Down** or Unlock doors on anti-passback areas (APBs) on demand
- **Simplifies Security Management -** Add or disable credentials/badgeholders; change settings & schedules, threat levels, manage personnel privileges
- **Built-in Credential –** Provides logged access via a customizable list of approved entry-points without a physical credential
- **Cost-Saving Universal Functionality -** Brand Agnostic App use with any lock or reader brand on CA4K System
- **Integrators' *Shake-Swap* Control between multiple clients'** hosted or remotely managed enterprise systems – ideal complement to comprehensive CI Dealer Program

Continental Access

Download on the App Store | GET IT ON Google Play

www.cicaccess.com | 1.800.645.9445

Continental Access, a Division of Napco Security Technologies, Inc.

CA4K, uniVerse™ and Trilogy Networx® are trademarks of Continental Access & or parent co. Napco Security Technologies Other marks remain intellectual property of their respective cos. Prelim data subject to change without prior notice.