

SECURITY MANAGEMENT

July/August 2021

Published by ASIS International



Open Secrets

Threats are evolving, but are corporate security intelligence methods keeping pace?

By Mark Ashford

CRITICAL INFRASTRUCTURE PROTECTION AND INCIDENT MANAGEMENT

Natural disasters, active assailants, political unrest, crime, and terrorism reflect the heightened need for coordinated preventive and response efforts and **critical incident management**. Protecting critical infrastructure demands planning, collaboration, and access to information. Geographic Information Systems (GIS) unifies security teams, supports the early detection of risk, and aids rapid response and incident closure—enhancing your ability to protect employees, customers, organizational assets, and the public.

SUSPICIOUS ACTIVITY

Nearest Facility: 0.2 mi
Total Employees: 23

ASSAULT

Nearest Facility: 0.7 mi
Total Employees: 35

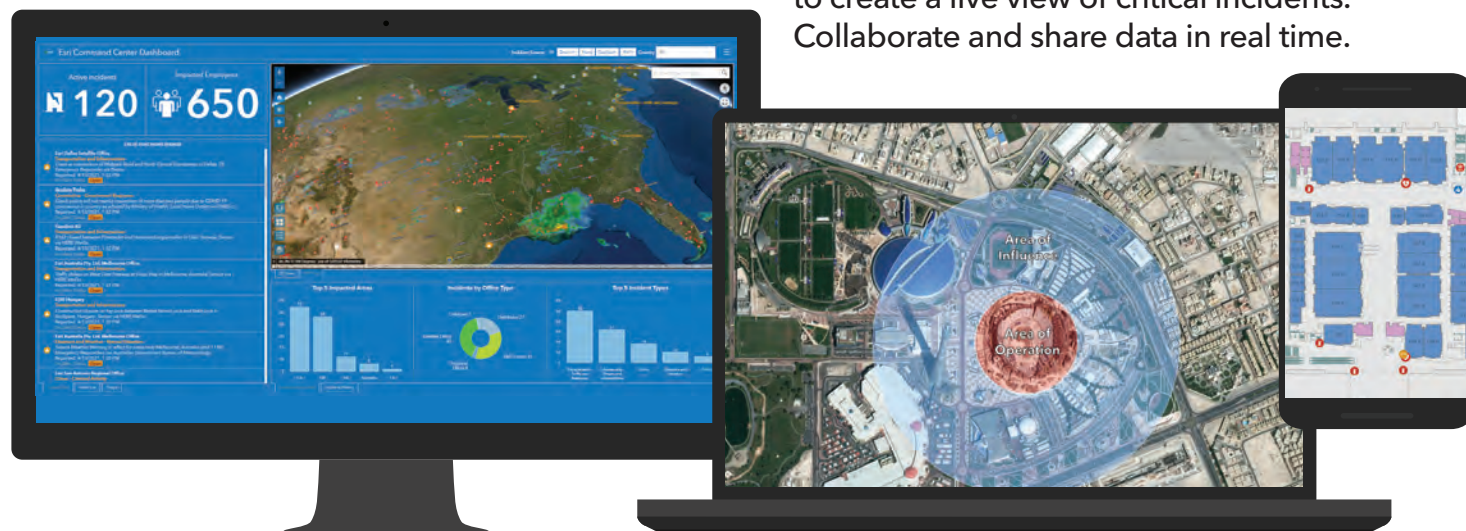


Reasons to Choose GIS for Your Site Security Operations

GIS is a framework for gathering, managing, and analyzing data in real time. ArcGIS® software from Esri integrates many types of data and security feeds, supports analysis in the context of location, and organizes layers of information using 2D and 3D maps and visualizations. With these unique capabilities, GIS reveals deeper insights into data—such as patterns, relationships, and situations—helping security personnel make smarter, faster decisions.

GIS can help your organization with the following:

- **Understand your area of operation (AOO)**—Protect critical infrastructure with powerful map visualizations and incident data that evolve with your event security needs.
- **Design operational pre-plans**—Leverage a fully integrated framework to guide the planning, preparation, and execution of security operations for critical incident management.
- **Build a tactical response**—Manage incidents with adaptable and configurable response plans. Build and modify security plans in real time to support an evolving tactical situation.
- **Deliver shared awareness and collaboration**—Integrate information from varied sources to create a live view of critical incidents. Collaborate and share data in real time.



Protect your employees, customers, and critical infrastructure.
Learn more about how GIS enables corporate security and safety.

Download our ebook:
go.esri.com/incident-management





Securing the peace.

**Campus police upgrade to
a smarter body worn solution.**



Hampered by slow video downloading and activation frustrations, the Campus Police Department of the Putnam City School District in Oklahoma wanted to replace their cumbersome 6-year-old body worn camera system. So, they turned to Axis Communications. The campus police officers love their new body worn cameras from Axis, particularly the simultaneous downloading and charging process, single tap activation, and video encryption. Check out their full story to see how the new solution has helped them dramatically streamline and improve operations.

Learn more at www.axis-communications.com/putnam


Contents Notable

“By understanding the needs of young employees, it is possible to tailor programs to meet these needs and retain talent.”

Jennifer Hesterman explains how mentorship programs present a myriad of unexpected benefits. [Page 42](#)

1997

The first year the U.S. Government Accountability Office placed government cybersecurity on its High-Risk Series. It remains on the list nearly 25 years later. [Page 22](#)



“The challenge of unreliable information, especially in today’s age of disinformation, is not insurmountable.”

Mark Ashford outlines the benefits and challenges of leveraging open-source intelligence (OSINT) for more dynamic threat assessments. [Page 31](#)

“All our staff—whether you’re an usher or a security guard or concession worker—will become health capacitors.”

Mario Coutinho, vice president of Stadium Operations and Security for the Toronto Blue Jays, predicts that COVID-19 will change the roles of stadium personnel and technology forever. [Page 48](#)

76

The percentage of U.S. employees who described themselves as currently “stressed,” which could result in higher levels of burnout and physical illness.

[Page 19](#)



1.1 M

The number of English-language articles published in a five-month period that contained misinformation about COVID-19. Mistrust in media only heightens the importance of corporate risk communications.

[Page 16](#)



Security Management (ISSN 0145-9406) Volume 65, Number 4, is published bimonthly by ASIS International, 1625 Prince St., Alexandria, VA 22314; 703.519.6200; fax: 703.519.6299. Subscriptions: ASIS members—\$60 for 1 year (included in dues, non-deductible). Nonmembers in US, Canada, and Mexico—1 year, \$60; 3 years, \$162. All others—air delivery—1 year, \$120. Bulk subscription rates available. Periodicals postage paid at Alexandria, VA and additional mailing offices. Mailed in Canada under IPM #0743968. Postmaster: Send address changes to ASIS International, Attn: *Security Management*, 1625 Prince St., Alexandria, VA 22314. *Security Management* is a registered trademark and its use is prohibited. Copyright © 2021 ASIS International, Inc. This information is protected by copyright and trademark 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.

Avoid Predictable Post-Occupancy Program Drift

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

Secure your tomorrow.

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

Download the case study: zbeta.com/drift

For product info #3 securitymgmt.hotims.com



ZBETA

Contents Features

JULY/AUGUST 2021

EXECUTIVE TEAM

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

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

Nello Caramat
publisher
Nello.Caramat@asisonline.org



1625 Prince Street
Alexandria, VA 22314
703.519.6200
fax 703.519.6299

MEDIA SALES

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

Femke Morelisse
Account Manager
Companies M through Z
703.518.1502
Femke.Morelisse@asisonline.org



COVER STORY

26 Open Secrets

Threats are evolving, but are corporate security intelligence methods keeping pace?
By Mark Ashford

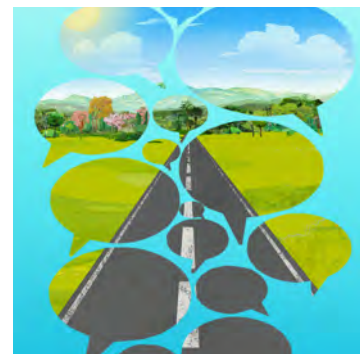


32

ORGANIZED CRIME

Profiting Off the New Abnormal

During a pandemic, the threat of organized criminal activity evolved to survive and take advantage of new business opportunities.
By Megan Gates

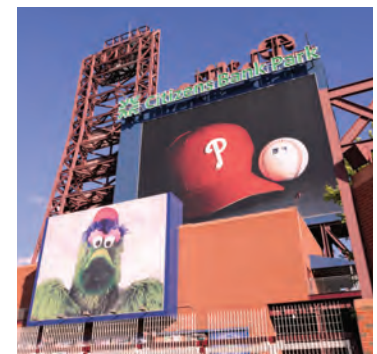


38

MENTORING

A Two-Way Street

COVID-19 has wreaked havoc on global workforces. To retain and foster future leaders amid the tumult, personal connection through mentorship can provide support and grow both mentor and mentee.
By Claire Meyer



44

SPORTS SECURITY

Ballpark Figures

Baseball stadiums strive to adapt their security postures and work with their communities to keep fans, players, and others safe, even when it's not game time.
By Sara Mosqueda

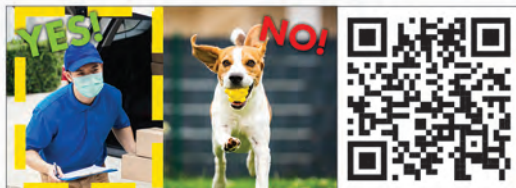
⚠ Alert: Human Detected!

Tired of **FALSE** motion alarms?
Speco is.

Speco's Human & Vehicle Detection ignores false triggers
and alerts you to motion that matters!



Speco's analytic cameras and recorders with **Human and Vehicle Detection** can notify you of people, cars, trucks, and bikes in the scene and ignore everything else such as animals and precipitation. Alarms can be triggered if the selected detector enters the view or a predefined region. Alarms can also be tailored to trigger upon entrance or exit of region.



Scan to see a quick Human & Vehicle
Detection **Feature Showcase Video**

For more information on these
Advanced Analytics and more visit specotech.com

Contents Departments

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

PRODUCTION & CREATIVE SERVICES STAFF

Tyler Stone
art director
Tyler.Stone@asisonline.org

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

Caitlin Donohue
assistant art director
Caitlin.Donohue@asisonline.org

Mariah Bartz
senior graphic designer
Mariah.Bartz@asisonline.org

SECURITY MANAGEMENT

1625 Prince Street
Alexandria, VA 22314
703.519.6200
fax 703.519.6299

MISSION STATEMENT

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

16

NEWS AND TRENDS

Trust Amid Misinformation

Trust in information sources and media hit record lows in 2021, but trust in employers remains high.

By Claire Meyer



20

CASE STUDY

Proactive Patrols

Campus security for the University of Regina is using a new software system to support both the university and its guard force.

By Sara Mosqueda



22

CYBERSECURITY

Cyber Catch-Up

Nearly 25 years after risks to federal information systems were flagged, the U.S. government may be poised to start addressing them.

By Megan Gates



62

LEGAL REPORT

Judicial Decisions

A Russian national pled guilty to conspiracy after attempting to pay a Tesla employee to introduce malware to the company's network.

By Sara Mosqueda



10

Contributing Authors

12

Online Exclusives

Diversity, equity, and inclusion (DE&I) are more than a business imperative—they are a matter of survival.

14

Editor's Note

When deliberating vital decisions, context matters.

50

Security Technology

Recent analysis found that there are already more than 770 million surveillance cameras in use worldwide, and 54 percent are in China.

52

ASIS News

The game has changed. So has GSX. Discover a new hybrid experience September 2021.

53

ASIS Global Board of Directors

55

Industry News

A remote monitoring program at a restaurant chain found that only 5 percent of alarms required police response.

By Sara Mosqueda

56

ISC West Product Showcase

64

Marketplace

65

Advertiser Index

66

Infographic

At the start of the pandemic, the FBI warned that it expected a surge in hate crimes against people of Asian descent. Recent data is proving that to be true.

Contributing Authors



Mark Ashford

SECURITY ANALYST

Mark Ashford works in security risk analysis and threat assessment within the financial industry, following a 12-year background in law enforcement as both a uniformed officer and appointed detective. Ashford also worked in state security. His educational background includes a bachelor's degree in Policing Studies, as well as having undertaken terrorism studies with the University of St. Andrews in the United Kingdom. Ashford has engaged in professional development courses with NATO and the European Union Agency for Law Enforcement Training (CEPOL), and he is a member of ASIS International. His other areas of interest include intelligence analysis, strategic foresight, and international relations.

"Open Secrets,"
Page 26



Ross Johnson, CPP

CRITICAL INFRASTRUCTURE CONSULTANT

Ross Johnson, CPP, is president of Bridgehead Security Consulting, Inc. Johnson is the co-chair of the Electricity Information Sharing and Analysis Center (E-ISAC) Physical Security Advisory Group, a member of the Critical Infrastructure Steering Committee at ASIS, and the author of *Antiterrorism Planning and Threat Response*.

Book Review,
Page 17



Joshua D. Fowler, CPP

CUSTOMS AND BORDER PROTECTION RED TEAM LEADER

Joshua D. Fowler, CPP, is a retired U.S. Air Force Security Forces officer with 28 years of antiterrorism, emergency preparedness, and law enforcement experience. He currently conducts worldwide red team testing of U.S. Customs and Border Protection (CBP) locations.

Book Review,
Page 23



Dennis Eberly

ON TARGET INVESTIGATION & CONSULTING, LLC

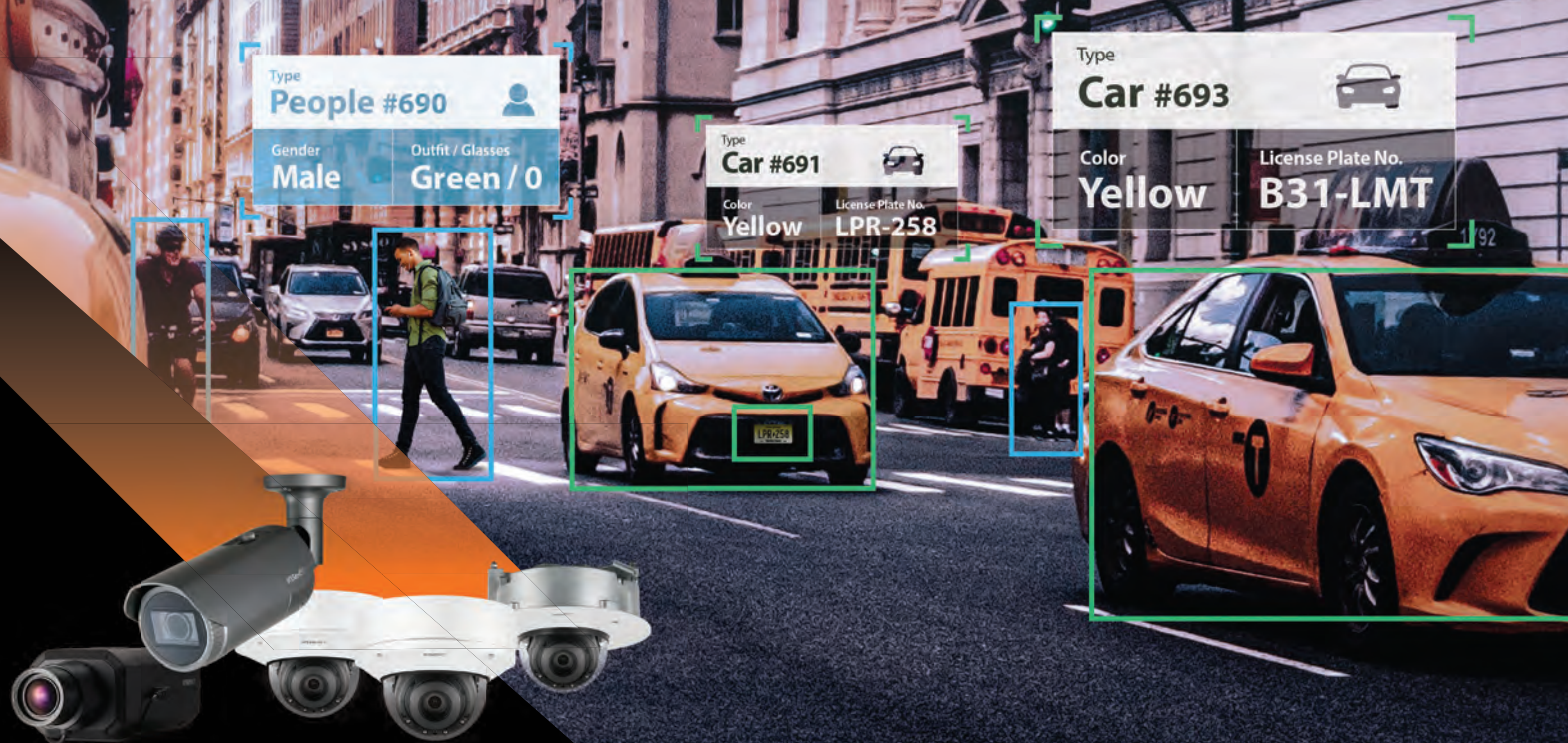
Dennis Eberly, M.S., LPI (Licensed Private Investigator), is the owner of On Target Investigation & Consulting, LLC. He retired as a lieutenant from the East Hempfield Township Police Department in Lancaster County, Pennsylvania, after 33 years of service. Eberly has held criminal justice faculty positions at several institutions over the past three decades.

Book Review,
Page 53



Wisenet AI

Reduce false alarms with Deep Learning technology.



Wisenet P series AI Cameras

Conventional cameras detect motion based on pixels alone. Hanwha Techwin's Wisenet P series cameras combine Artificial Intelligence algorithms and Deep Learning technology to create event alarms only for people and vehicles, reducing false alarms and enhancing operational efficiency. Filter out irrelevant movements caused by waving trees, shadows or animals. Generate only the events you need to see for effective forensic searches.

That's the power of Wisenet AI.

HanwhaSecurity.com

© 2021 Hanwha Techwin America

For product info #5 securitymgmt.hotims.com



Online Exclusives

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



Fostering the Geniuses in Your Backyard Through DE&I Efforts

By Claire Meyer

Diversity and inclusion bring myriad benefits to organizations, from unique perspectives in crisis management to fostering future talent to building a more resilient culture. Diversity, equity, and inclusion (DE&I) are more than a business imperative, however, they are a matter of survival, says James Pogue, PhD, an educator and speaker on diversity and CEO of JP Enterprises.

“When you talk about inclusion and how it brings value, it’s about relevancy,” he says. “Do you want to exist? Do you want your business to thrive? Do you recognize that by precluding the inclusion of inclusive business practices that you are relegating yourself to a second-tier, third-tier, or fourth-tier set of opportunities?”

The talent pool of people who are “just like me” is limited, Pogue adds, and recruiting within that homogeneous group not only limits an organization’s prospects—it limits the organization’s ability to manage a diverse and rapidly changing landscape.



Risk Assessment Approaches for Reopening of Cultural Venues

By Andy Davis, CPP

Slowly, global cultural and heritage sites are starting to reopen to the public. As part of that reopening process, it is important for those responsible for securing artifacts, visitors, and venues to ensure that their security risk management approach remains viable. The cultural and heritage sectors have been severely impacted by forced closures and loss of revenue; not all are centrally funded, and some, unfortunately, have been forced to close for good.

For those cultural properties that could reopen, the social environment in which the world is operating has changed irreversibly—at least in the short to medium term. The context in which the previous risk assessments were—or should have been—undertaken is different. Therefore, the threats that are faced and the risks they pose by default have also changed.



Enabling Agile Decisions in an Evolving Risk Environment

By Lianne Kennedy-Boudali

We are in a period of significant change in the global risk environment. These changes—which include an exponential increase in signal data, greater focus on the role of corporations in civic and political affairs, social unrest, and rapid globalization of local events—have required security leaders to adapt their risk analysis process accordingly. Many have discovered that, due to the pace of change and increasing demands for real-time risk analysis, organizational capabilities that were effective five years ago are no longer sufficient in today’s environment.

The ability to respond effectively depends on having the right information at the right time, and agile decision-making requires that business leaders support risk analysis by registering risks to their organization, building proactive teams, and effectively leveraging data and technology.



How to Avoid Pandemic-Related Litigation Risks

By Rita Zeidner

Worries over workplace safety in the COVID-19 era, as well as concerns about the impacts of business closings, plant shutdowns, and mandatory stay-at-home orders, spawned more than 2,000 lawsuits in the United States from January 2020 through March 2021, according to Atlanta-based employment law firm Fisher Phillips.

Complaints have included unsafe-workplace allegations, as well as grievances about the handling of layoffs, furloughs and recalls; remote work arrangements; and leave requests.

Some states have enacted legislation blocking COVID-19-related claims against employers, but these laws do not prevent federal lawsuits.

The current case inventory may be just the tip of the iceberg, since many workers whose livelihoods were negatively impacted by the public health crisis may still be considering whether they have options for legal redress, says attorney Gerald Maatman, Jr., a partner at Seyfarth in Chicago.



Using Puns to Promote Security Awareness

By Megan Gates

Travel is coming back. On 28 April 2021, 1.18 million travelers passed through a U.S. Transportation Security Administration (TSA) checkpoint compared to 119,629 on the same day in 2020 and 2.26 million in 2019.

With that resumption in travel, however, may come anxiety and uncertainty about what's allowed to pass through a TSA checkpoint at the airport. And for security practitioners themselves, some may be wondering how best to share updates with travelers and visitors so they can prepare accordingly.

According to Emily Bonilla-Pieton, social media lead for TSA, the agency uses its celebrated Instagram account to communicate with nearly 1 million followers about essential security information through puns, dad jokes, and K9 pictures. In an interview with *Security Management*, she shared security awareness lessons learned, tips, and a peek into the planning process behind each post.



Human Trafficking Intervention; Casino Security; and Connected Devices

Hosted by Chuck Harold

Lauren Shapiro outlines recent U.S. human trafficking liability updates and private security's role in helping victims; Derk Boss, CPP, shares how casino security has changed since the beginning of COVID-19; and Elisa Costante breaks down three big challenges in connected devices.

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

TRENDING News & Analysis

Cybersecurity Executive Order

U.S. President Joe Biden signed an executive order demanding improvement in federal system security.

Climate Change

A scientific study found that human-caused climate change was responsible for \$8 billion of the damage caused by Hurricane Sandy in 2012.

Resisting Ransomware

A task force recommended 48 actions to mitigate the threat of ransomware, including regulating cryptocurrency.

Daily news available at asisonline.org/TodayInSecurity.

SOCIAL MEDIA

KEEP IN TOUCH

 @SecMgmtMag

 @SecMgmtMag

 ASIS International




STRIKE SECURITY

THERE ARE MANY THINGS TO CONSIDER BEFORE DURING AND AFTER A STRIKE.

Putting it all together takes knowledge, experience and dedication.

Special Response Corporation is a national leader in providing highly specialized security services. With over 30 years of experience meeting the labor crisis security needs of more than 2,000 clients in the U.S. and Canada, we can help minimize costly disruptions to your business resulting from a labor dispute. Our teams consist of professional, disciplined and highly trained security personnel with extensive law enforcement or military experience. They are on stand by status and can be deployed to your location with 24 hours notice or less. When you need help during a labor dispute, call on Special Response Corporation for complete, professional support.

Special Response Corporation
Protecting business, industry and government throughout North America for over three decades.
Contact Us • Anytime! 410 • 785 • 1212
www.specialresponse.com

CONTEXT MATTERS

The truth sometimes relies not on fact, but on context. This is crucial to comprehending how facts and statistics influence our lives and in determining whether these measurements add value to our understanding of the world, according to Tim Harford's new book, *The Data Detective*. As a thought experiment, Harford suggested thinking about how daily news outlets report the news as compared to magazines. "Bloomberg might pick up on sharp market moves over the past hour. The same moves won't merit a mention in *The Economist*," he noted.

Harford next invited readers to imagine news during a much longer period of time—decades, or even centuries. What would the headlines be? A newspaper published in 2018 covering the past 50 years might be a declaration of something that never occurred: "Phew! World Avoids Nuclear Armageddon!"



Actionable intelligence is ubiquitous, but it must be approached through analysis and assessment.



A reader from 1968 would consider this incredibly newsworthy. Harford wrote: "It would be big news that the Cold War had simply ended without a nuclear exchange of any kind—even if no daily newspaper would have been tempted in the meantime to run with the headline 'No H-Bombs Dropped Today.'"

The 100-year headline—"Child Mortality Falls by a Factor of Eight"—and the 200-year headline—"Most People Aren't Poor"—bear little resemblance to the issues we regularly ponder because the news that catches our attention is surprising, negative, and often misleading.

In this month's cover story, "Open Secrets," author Mark Ashford discusses how open-source intelligence (OSINT) can provide valuable information to security professionals if approached in the correct context. Ashford, who specializes in risk analysis in the financial industry, notes that actionable intelligence is ubiquitous, but it must be approached through analysis and assessment.

As evidenced by numerous global events that captured comments, details, and even changes recommended to accommodate space for signature below photos on social media, OSINT can be useful in making security decisions, but pitfalls abound. Ashford notes that OSINT must be an active process, not a one-time collection of data.

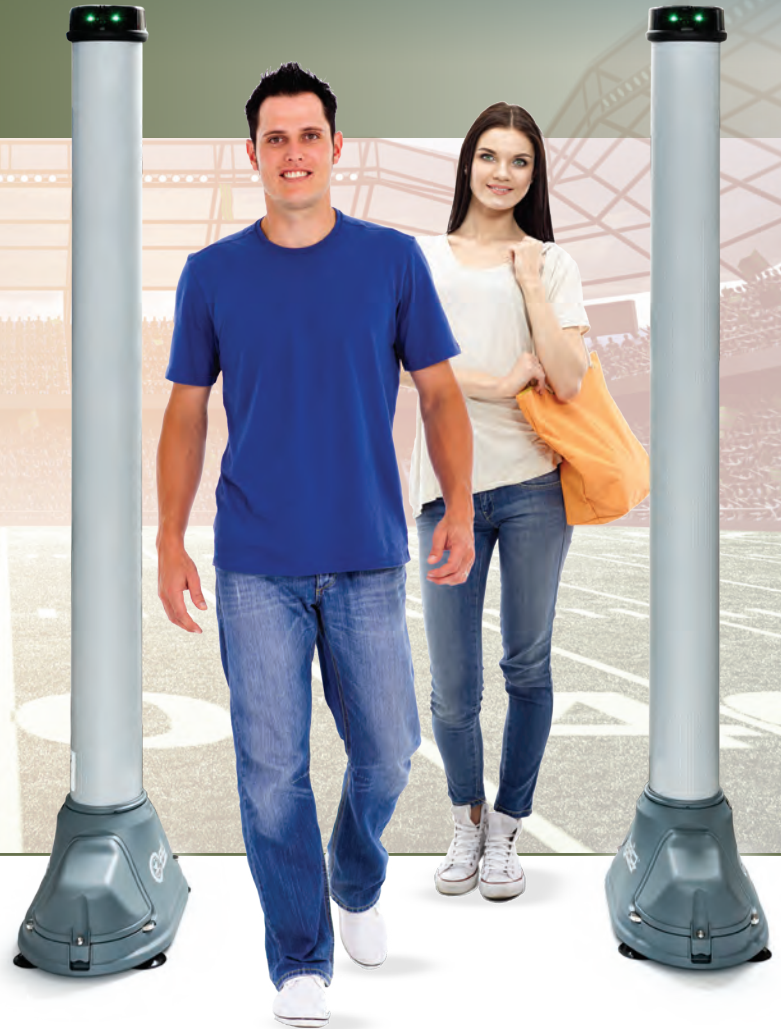
"There is a need to regularly and actively re-evaluate intelligence as new questions arise, assumptions are challenged, and new information comes to light," he writes.

Ashford also warns about the threat of bias in making assessments about OSINT. Biases, he adds, "can lead to the wrong conclusions, so the information, our views, and our statements should constantly be challenged to identify what is actually important."

Determining what is actually important to security professionals is a key mission for ASIS International and *Security Management*. And context is key in our coverage, meaning that stories are delivered differently depending on the type of information. For the news of the day, we continue to expand our digital offerings to provide more timely stories and online exclusives. In-depth articles that require research and analysis will remain in the pages of the print magazine to provide context straight from your bookshelf for years to come. ■

Teresa Anderson
Editor-in-Chief
Teresa Anderson

GAME DAY AT RECORD SPEED.



OPENGATE™ (NEW) *Groundbreaking Weapons Detection System*

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

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

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

Trust Amid Misinformation

Trust in information sources hit record lows in 2021, but trust in employers remains high. Security now has an opportunity to help rebuild confidence in organizations through effective communication.



By Claire Meyer



Misinformation had a banner year in 2020, and it continues to rise. A 2020 study from the Cornell Alliance for Science of 38 million articles about the COVID-19 pandemic in English-language media worldwide in the first five months of 2020 found that more than 1.1 million contained misinformation ranging from mere mistakes to conspiracy theories to dangerously misleading or false statements about potential treatments and miracle cures.

Misinformation has the potential to cost lives, the report's authors said. If people are misled by unsubstantiated claims about the disease, they are less likely to observe official

When the government is absent, people clearly expect business to step in and fill the void.

health advice—putting themselves and others at risk of the spread of COVID-19. In addition, “health protection strategies such as hygiene, sanitation, social distancing, mask wearing, lockdowns, and other measures will be less effective if distrust of public health authorities becomes sufficiently widespread to substantially affect public behavior,” according to the report.

Exposure to fabricated news or misinformation also leads to general distrust in political institutions and media organizations. A Harvard Kennedy School study found that exposure to misinformation—particularly fake news delivered through a divisive or sensa-

Risk communications is about allowing the audience to make its own decisions.

tional lens—in a one-month period around the 2018 U.S. midterm election resulted in a 5 percent decrease in media trust.

“The consequences of this lack of trust are especially apparent in times of crisis and uncertainty when citizens are most in need of credible sources providing current and reliable information,” according to the report. “To the extent that fake news can undermine the public’s confidence in mainstream media, it may not only leave its consumers misinformed, but also make them more vulnerable when disaster strikes.”

Trust in information sources across the board hit record lows in 2021. According to the 2021 *Edelman Trust Barometer*, trust in traditional media dropped eight points from 2020, with only 53 percent of survey respondents looking to it for reliable information. Social media and owned media dropped even lower—just 35 percent and 41 percent of respondents, respectively.

But there is a glimmer in this dark cloud of mistrust. The 2021 *Trust Barometer* found that business is the most trusted institution—globally, 61 percent of people trust information from business—and among the four institutions studied (business, NGOs, government, and media), it was the only one seen as both ethical and competent.

“When the government is absent, people clearly expect business to step in and fill the void, and the high expectations of business to address and solve today’s challenges has never been more apparent,” according to the report.

More than 85 percent of respondents agreed that CEOs should publicly speak out about societal challenges, and 68 percent said CEOs should step in when government does not fix societal problems. More than three-quarters of respondents said that they trust their employer. More than half of survey respondents (53 percent) said that when reliable news media is absent, corporations have a responsibility to fill the information void.

To maintain this trusted position, businesses need to guard information quality, ensuring that trustworthy information goes out to employees and the community, the *Barometer* said.

But during a crisis—whether a macro-crisis that affects a broad audience, like a natural disaster, or a micro-crisis within an organization or department, like an insider threat—security is often an integral part of a business’s response. Therefore, security professionals need to be prepared to participate in communication efforts, says Ernest DelBuono, a crisis management consultant and member of the ASIS Crisis Management and Business Continuity Community Steering Committee.

“You need to understand communications because your corporate communications are an important part of any type of security issue you may have,” he says. “As a security professional, if you can’t understand how the communications system works, it’s going to be

hard for you to convince the communicators where they need to go.”

Or if security tries to be protective and lock down any information about an incident from spreading, it won’t stop people from communicating about the incident on their own—often with erroneous information, or relying on outside reporting or opinion about the organization.

“Meanwhile, we’re losing market share, we’re losing reputation, because we’re not saying anything,” he adds. “Silence doesn’t help. You’ve just given up control of the narrative.”

Instead, DelBuono recommends forging early and frequent partnerships with counterparts in communications departments to embed security in crisis management and

Book Review

The Professional Protection Officer

Edited by Sandi J. Davies and Lawrence J. Fennelly. Butterworth-Heinemann; Elsevier.com; 546 pages; \$59.95.

The duties of today’s professional protection officer are complex. They can be found conducting a wide range of activities: loss prevention, fire prevention, traffic control, access control, active shooter prevention and response, and emergency management—to mention just a few.

The one single factor whose presence or absence can predict the success of a professional protection officer is training. Diverse training requires diverse resources, however, and that can be prohibitively expensive.

The Professional Protection Officer: Practical Strategies and Emerging Trends provides an up-to-date collection of the knowledge and skills required of protection officers in today’s environment. It is readable, organized, and should be issued to all protection officers by their employers as an investment in the officers’ and their companies’ futures.

The book is organized into three parts: foundational knowledge that applies across the security profession; practical and operational concepts—which provide details on specific tasks or issues, such as traffic control, officer

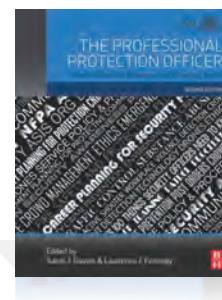
safety, use of force, or patrol principles; and career development.

Protection officers who read and use the information and concepts in this book will provide superior performance. They will impress clients and enhance their employer’s reputation. They will also be exposed to a wide array of subjects, such as emergency planning, UAV operations, HAZMAT, and information security.

This is the second edition of this book, and it serves as a good signpost showing where the industry is today. As anyone who has attended GSX can tell you, the security industry is going through a technological and doctrinal revolution of its own, with automation and artificial intelligence pushing us into the future.

This book is strongly recommended for protection officers at any career stage, their managers, and security professionals who need or use their services.

Reviewer: Ross Johnson, CPP, is the president of Bridgehead Security Consulting, Inc. He is the co-chair of the Electricity Information Sharing and Analysis Center (E-ISAC) Physical Security Advisory Group and is the author of Antiterrorism and Threat Response: Planning and Implementation.



communications protocols. He also suggests positioning security leaders as internal subject matter experts and potential spokespeople—especially for security topics like workplace violence incidents.

Effective messaging depends on determining the correct audience and selecting the right representative to deliver messages. But this is not always the CEO, DelBuono cautions—crisis communication models often recommend selecting speakers based on credentials and qualifications instead of organizational position. In a health crisis, for example, the company could present information from its chief health and safety officer, who could walk employees through developments and safety measures as the crisis unfolds.

Despite business ranking highest on the 2021 *Trust Barometer*, trust in information from authority figures is still low all around. Even if an organization handled the many crises of 2020 well, it exists in a world rife with polarization, conspiracy theories, and mistrust, says Helio Fred Garcia, a professor of crisis management at New York University and

president of Logos Consulting Group. A societal lack of trust requires businesses to take additional steps to shore up employees' and stakeholders' confidence in their statements and competence.

The key to developing—or rebuilding—trust is to make good on your promises, Garcia says. However, it cannot stop there. After the company makes a declaration of its commitment, it must deliver on that promise, remind people that it made a promise and met it, and then repeat the process frequently and vocally.

And these promises don't need to spring from an ambitious shift in company strategy or mark the completion of a multi-year project, either.

"On all the things you know you're going to do anyway, turn each of them into a promise," Garcia says. "And if there are five steps to any one of those things, make that five promises."

After people are regularly reminded of how they can trust the business to meet its obligations, trust begins to grow and solidify, he adds.

During a crisis, promises may need to be curtailed. DelBuono advises that crisis communications start early, stay open and trustworthy, and only promise that leaders will do their best. Situations can change quickly, rendering early pledges obsolete or unfeasible, but the audience may not understand the context and only see that the organization failed to meet expectations, he says. It may even be worthwhile to add a disclaimer to press releases issued during a crisis explaining that as more facts emerge, information may change.

However, this does not always address the challenge of misinformation. "We can't persuade the unpersuadable," Garcia adds. Misinformation often serves the role of people making sense of existing grievances, becoming a form of confirmation bias.

"One reason it is so hard to get people off of misinformation is because it makes sense for them, connecting their grievances in a common cause," he adds.

Consider conspiracy theories about microchips in vaccine doses. People are already anxious about vaccines and the COVID-19 pandemic, so they may use rumors and misinformation to justify their fears. However, like rumors, these justifications spread and they amplify as they proliferate.

This can impact the workplace in a number of ways, Garcia adds. Increased division along differences in belief systems or conspiracies can foster an "us vs. them" mentality, which can result in conflict in the workplace.

Misinformation often serves the role of people making sense of existing grievances, becoming a form of confirmation bias.

"There's this clash of worldviews that puts people's safety and lives at risk," Garcia says. "Now what does this do to trust? You end up trusting your own team, and distrusting the other team."

While different belief systems will always exist in the workplace, Garcia says the key in turbulent times is to declare and enforce a set of clearly defined values or protocols, such as demanding that employees treat each other with respect, and imposing consequences for disrespect. Being clear and up-front from the start helps people to know where they stand within the workplace, how they should model their behavior, and what information to expect from their employer.

"Risk communications is about allowing the audience to make its own decisions—about whether to go out in public, to use this product, to stop using this medication," DelBuono says. "Particularly in a crisis, people want to know not so much that you've solved the problem, but what action you are taking as an organization."

Stressed About Wellness

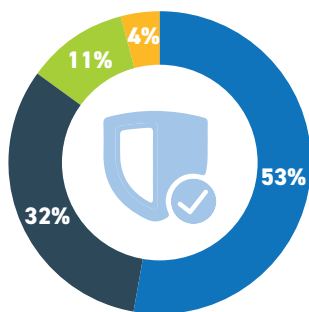
U.S. workers rank mental and psychological wellbeing as one of their biggest wellness concerns, but participation in programs like mental health resources or Employee Assistance Programs (EAPs) has dropped, according to a March 2021 survey from The Conference Board.

Among more than 1,100 U.S. workers across industries and positions, 59 percent of people ranked mental and psychological wellbeing—such as stress or burnout—as one of their top three concerns, followed by physical wellbeing (36 percent), social wellness and belonging (36 percent), professional wellbeing (27 percent), and financial wellbeing (21 percent).

Among lower-level employees, 76 percent were concerned about mental wellbeing, compared to 53 percent of CEOs.

Lacking Control

Most Americans said increasing staffing and resources for border patrol and police is important for addressing the situation at the U.S.-Mexico border.



■ Very important ■ Not too important
■ Somewhat important ■ Not important at all

Source: *Most Americans are Critical of Government's Handling of Situation at U.S.-Mexico Border*, Pew Research Center, May 2021

Stress is a widespread problem. The 2021 *Working Americans' State of Stress* report found that 76 percent of workers described themselves as currently "stressed," and 46 percent said their stress levels were moderate or higher.

The Conference Board survey said that age and gender factored into well-being concerns, with Millennials most concerned about mental and psychological wellbeing and Gen X workers more concerned about social wellness and belonging. Women were more concerned about spiritual wellbeing—feeling a sense of purpose in what they do—while men were more concerned about social wellbeing.

Stress levels vary by age as well. The *State of Stress* report found that while only 67 percent of workers over 60 years of age reported significant stress, this rate increases steadily across younger demographics until it reaches the youngest bracket of workers aged 18 to 29—84 percent of whom reported high stress levels.





Stress can result in physical and mental problems, including physical illness or fatigue (51 percent); inability to concentrate, anxiety, depression, or burnout (56 percent); and sleep disruption or ineffective sleep (55 percent), the report found. It also results in changes of behavior; 48 percent of workers reported increased consumption of unhealthy foods, 42 percent reported decreased physical activity, and 25 percent reported increased use of alcohol or controlled substances.

Despite concerns about stress and burnout, participation in mental health resources and EAPs dropped four percent during the pandemic, The Conference Board found. Usage of online resources or tools increased six percent, however, and Millennials in particular increased their use of online resources by 19 percent. Community wellbeing programs took the largest hit—25 percent fewer U.S. workers reported using these programs, which provide time off for volunteering.

Leaders are largely doing well when it comes to supporting their employees. The survey found that 78 percent of workers believe their supervisor genuinely cares about their employees' wellbeing, and 62 percent said they feel comfortable speaking about wellbeing challenges at work. Nearly one-fifth of workers, though, do not feel comfortable discussing their hardships for fear of negative consequences, and women are more likely to be uncomfortable than men. ■

BARRIERS & SECURITY BOLLARDS





Protecting what
MATTERS MOST.



AMERISTARSECURITY.COM
866-467-2773

AMERISTAR®
ASSA ABLOY

ASSA ABLOY, the global leader
in door opening solutions

For product info #8 securitymgmt.hotims.com

Proactive Patrols

Campus security operations for the University of Regina in Saskatchewan, Canada, is using a new software system to support both the university and its guard force.



By Sara Mosqueda



We had to make a decision because certain things weren't getting supported anymore.

In many ways, 2019 was a typical year for the University of Regina. Its student body of roughly 16,500 students was living in dorms and learning in lecture halls or labs on the campus, nestled within Regina, Saskatchewan, Canada. Similarly, the university's 2,000 employees worked on site and in-person—including the security team.

But today, like many other establishments of higher education, classes and work are largely conducted online, even for some security roles. The University of Regina campus and its various departments are preparing to reopen to 50 percent capacity come September 2021, and if another wave of new COVID-19 cases doesn't derail the progress, a full reopening is scheduled for January 2022.

In the meantime, Scott Crawley, manager of campus security operations, can safely work from home while keeping tabs on developing issues on campus with real-time information coming in through the university's incident reporting software. And just because the campus is locked down to avoid spreading the coronavirus, it doesn't mean all remains quiet.

In 2019, students and staff filed a total of 1,225 reports about incidents—ranging from vandalism to sexual assault—which required the security team to follow up or investigate the issue. In 2020, that number dropped down to 806 security incidents.

However, the number of total calls for service jumped from 13,633 to 19,640. Some of that increase was due to more information calls. For example, a limited number of access points were established for people approved to use the university's facilities. Students and staff would check in at these access points, enabling the university to track the number of people entering the campus and the areas they would work in. So, if a COVID-19 hotspot developed on campus, university staff and security would be able to notify anyone who may have been exposed to the virus. Crawley says that several calls came from these access points—including requests for information, for assistance if an unauthorized person was trying to enter the campus, or if the entrances needed more masks, hand sanitizer, or wipes.

Before 2020, Crawley says he knew that campus security's record-keeping software and record-sharing system (which involved printing out the report, copying it, and physically sending it to other departments), while decent, could be better. "We had to make a decision because certain things weren't getting supported anymore," he adds.

Patrols are not the only proactive element of the systems—the trend reports also enable smarter security decisions.

While looking for alternatives, Crawley and his department came across Resolver's Incident Management and Command Center software programs. But the products would have exceeded the allotted security budget for just maintaining and sharing records. To get buy-in for the Resolver system, Crawley pitched to the university that it could be used by the security team, HR, and other departments. Although each group has access to the system, access to the files is determined by the user's privilege level and department.

The programs are used by campus security; health, safety, and wellness; student conduct; respectful workplace, which falls under the umbrella of human resources; and sexual violence. Although both software programs come as out-of-the-box solutions, Resolver worked with the different departments to customize their respective interfaces. It created specific forms and workflows, bringing the systems online at the beginning of December 2019. "They built it around our needs," Crawley says.

Campus security officers use Command Center as a dispatch module to coordinate and streamline their patrols. From the computer screen, a dispatcher in the security office is notified about officers' locations while on duty, specifically showing the time and location of the last call the officer responded to, as well as whether he or she is on a break or available to take an incoming call.

Crawley says that the university is also working on bringing a connected smartphone application online, which would be coordinated through Command Center. The app would allow dispatchers to track officers' locations in real time to quickly determine which officer is closest to an incoming call and which route to take to the scene. Officers will also use the app to indicate when they are on the scene, as well as directly upload photos related to the incident that can be compiled in a final report.

The dispatcher can file a report in the Incident Management program. The management system is also tied to the university's online portal for reporting issues, which gives the

person submitting the report the option to remain anonymous.

Members of the security team will triage the report, determining if they should continue investigating the issue or if the incident would be better handled by another department. If security does continue to investigate, officers conduct interviews (these days via Zoom) and leverage resources from other departments—such as the student record database.

Security operations managers and supervisors have access to the reports and can approve them through the Incident Management system, whether they are on campus or working from home. They can also notify investigating officers if more information is required.

Once a report is approved by a second supervisor, other relevant departments are notified. And if those departments need additional clarification or more information, the request is as easy as sending an email—a big change from the old method of printing out reports, which were then copied and physically sent to other relevant groups. Now, everything is saved in a cloud server, and sharing a file with the right people just involves selecting the correct online distribution route.

A large part of security's role has shifted since both the pandemic and the installation of the systems. Crawley says that his team is mostly involved in "proactive patrols," enabled through the trends reports that the software can generate to give insight into days and areas that are more likely to be the site of an incident on campus.

Crawley can pull a snapshot of the past 24 hours, including the number of calls for service and actual incidents within that timeframe. He can then compare days that featured a higher number of security incidents. "I know how many calls for service and how many incidents were created out of that 24 hours just with one click of a button," Crawley says.

The trend reports serve multiple purposes, both for justifying future budgets and driving scheduling decisions. "I kind of overlay all that, and it helps me with staffing as well," Crawley says. "It might mean someone getting a vacation day versus not getting one if it's a peak time."

Patrols are not the only proactive element enabled by the systems—the trend reports also enable smarter security decisions, Crawley says.

For example, 16 officers usually staff the security patrol team, but the recent departure of two officers created additional strain. Crawley

says that the systems helped him obtain buy-in to refill those positions.

He used reports to show the different kinds of incidents patrolling officers were likely to face and why they need additional resources. An officer responded to a break-in and attempted theft of construction equipment and tools on a satellite campus. That officer's only backup was the dispatcher, however, meaning that while both officers dealt with the issue, the dispatch desk was left unmanned and a report on the incident could not be filed until after the dispatcher returned.

While Crawley says he understands he will not see four teams of four patrol officers again until things start to pick up on campus, he adds that he knows that these reports emphasize how officers maintain safety throughout the campus and how the university administration can support them. ■

For more information about Resolver, contact Isaac Trask, Isaac.trask@resolver.com.

GSX
GLOBAL SECURITY EXCHANGE

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

UP YOUR GAME

With GSX Pre-Conference
Certification Review
Sessions.

CPP
PSP

gsx.org/pre-cons

Cyber Catch-Up

Nearly 25 years after a government watchdog began highlighting risks to federal information systems, the U.S. government may be poised to start comprehensively addressing them.



By Megan Gates



*Incremental improvements
will not give us the
security we need.*

It's been a rough year for those responsible for U.S. government network security. First, cybersecurity operators were notified that SolarWinds—a popular service used by government agencies and contractors alike—was compromised in a major supply chain attack that provided Russian actors access to sensitive information as part of an espionage campaign.

Then, in March, Microsoft called out China for taking advantage of a vulnerability in the company's Exchange email program to hack into organizations around the globe. And in April, cybersecurity firm Mandiant accused China of orchestrating a series of compromises to a Pulse Secure, LLC, program. U.S. federal government employees use this program to remotely connect to agency networks.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) released an alert on the Pulse Secure compromise, saying that since June 2020 it affected government agencies, critical infrastructure entities, and other private sector organizations.

"The threat actor is using this access to place webshells on the Pulse Connect Secure appliance for further access and persistence," according to CISA. "The known webshells allow for a variety of functions, including authentication bypass, multi-factor authentication bypass, password logging, and persistence through patching."

CISA mandated that all civilian agencies scan their systems to see if they were impacted by the Pulse Secure compromise and to take actions to address it. This mandate marked the second time in just seven weeks that the agency issued an emergency directive to take action to secure federal networks. Prior to 2021, CISA issued just three emergency directives in 2020 and one in 2019.

"Over the last year, CISA has issued several alerts urging agencies, governments, and organizations to assess and patch Pulse Connect Secure vulnerabilities," said Acting CISA Director Brandon Wales in a statement. "This emergency directive reflects the seriousness of these vulnerabilities and the importance for all organizations—in government and the private sector—to take appropriate mitigation steps."

The cascade of cybersecurity compromises highlights an ongoing problem that was first noted in 1997 by the U.S. Government Accountability Office (GAO), when it placed information systems security weaknesses on its High-Risk Series, an annual assessment of high risks to the U.S. federal government.

“These weaknesses pose high risk of unauthorized access and disclosure or malicious use of sensitive data,” GAO explained in the assessment. “Many federal operations that rely on computer networks are attractive targets for individuals or organizations with malicious intentions. Examples include law enforcement, import entry processing, and various financial transactions.”

The GAO highlighted that U.S. defense systems may have experienced roughly 250,000 attacks from hackers in 1995, with roughly 64 percent of them being successful and most going undetected.

“Since June 1993, we have issued over 30 reports describing serious information security weaknesses at major federal agencies,” GAO wrote. “In September 1996, we reported that, during the previous two years, serious information security control weaknesses had been reported for 10 of the 15 largest federal agencies. We have made dozens of recommendations to individual agencies for improvement and they have acted on many of them.”

But the U.S. government has not implemented hundreds of other GAO recommendations, and has often failed to move at a rapid pace when addressing cybersecurity at civilian agencies. That could finally be changing.

In May, U.S. President Joe Biden signed an executive order to begin overhauling the U.S. government’s cybersecurity and lay the groundwork for future improvements and outreach to the private sector.

“Incremental improvements will not give us the security we need; instead, the federal government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life,” the executive order said. “The federal government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises, or hybrid. The scope of protection and security must include systems that process data (information technology) and those that run the vital machinery that ensures our safety (operational technology).”

The executive order instructs agency heads to take numerous steps that fall into seven overarching categories: removing barriers to threat information sharing between government and the private sector; modernizing and implementing stronger cybersecurity standards in the federal government; improving software supply chain security; establishing a Cybersecurity Safety Review Board; creating a standard playbook for responding to cyber in-

We’re sitting at 25 years that GAO has been calling cybersecurity one of the highest risk areas to the nation.

cidents; improving detection of cybersecurity incidents on federal networks; and improving investigative and remediation capabilities.

Many of the action items touch on addressing vulnerabilities that malicious actors used to compromise federal networks. For instance, the executive order creates baseline security standards for the development of software sold to the federal government along with requirements for developers to maintain greater visibility into their software. It also requires

service providers to alert agencies they have contracted with about any cyber incidents—or potential incidents. These mandates address some of the vulnerabilities that were brought to light during the SolarWinds incident.

Along with these processes, the executive order also requires the U.S. federal government to implement security best practices.

“Outdated security models and unencrypted data have led to compromises of systems in the public and private sectors,” according to a White House fact sheet on the executive order. “The federal government must lead the way and increase its adoption of security best practices, including by employing a zero-trust security model, accelerating movement to secure cloud services, and consistently deploying foundational security tools such as multi-factor authentication and encryption.”

Book Review

Critical Infrastructure Risk Assessment

By Ernie Hayden, PSP. Rothstein & Associates, Inc.; Rothstein.com; 364 pages; \$74.99.

Ernie Hayden's *Critical Infrastructure Risk Assessment: The Definitive Threat Identification and Threat Reduction Handbook* is a comprehensive work that clearly provides the reader with details from foundational authoritative documents about U.S. critical infrastructure, including various executive orders, congressional laws, and presidential directives.

Hayden gives an international perspective from a handful of key industrial nations, and he clearly highlights shared dependencies and similarities. The book does a thorough job of explaining the various components of critical infrastructure, risk, and risk management well enough to enlighten someone new to the subject or to reinforce the knowledge of a skilled security specialist.

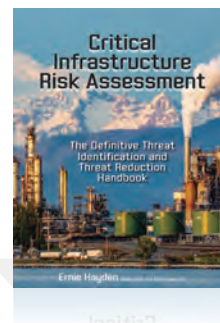
The bulk of the book covers the process of conducting a risk assessment and provides excellent outlines for the performance and documentation of the assessment. Hayden provides clear details of risk assessment methodologies so that the reader can clearly identify the dif-

ferences and determine which methodology is most applicable for specific assessments.

The book describes the requirements of conducting a pre-assessment, observation criteria, on-site actions, and the steps to conducting the final report. Of special note is the sample risk assessment report, which provides a clear example of a complete assessment report—complete with pictures and format outlines for the reader’s use.

The author achieved his intended goal of providing a template for conducting a risk assessment. This book is clearly formatted and organized for easy reference use, and its logical and beneficial construction is worthy of use by every security specialist, whether practitioner or consultant.

Reviewer: Joshua D. Fowler, CPP, is a retired U.S. Air Force Security Forces officer with 28 years of antiterrorism, emergency preparedness, and law enforcement experience. He currently conducts worldwide red team testing of U.S. Customs and Border Protection locations for chemical, biological, radiological, nuclear, and explosive (CBRNE), fraudulent document, human smuggling, and narcotics threats.



Most of the 16 agencies it reviewed had incident response processes with “key shortcomings” that limited their ability to minimize damage from attacks.

In addition to improving security, the executive order mandates touch on many of the problems that the GAO has identified in its assessments that have long been overlooked.

“We’re sitting at 25 years that GAO has been calling cybersecurity one of the highest risk areas to the nation,” says Nick Marinis, director, information technology and cybersecurity, at GAO. “And in some ways, the difficulty here is that it’s not only evolving—it’s getting bigger in the challenges and threats that our country and the world are facing from cyber-space attacks.”

Some of these threats were highlighted in the report that Marinis’ team published in March 2021, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, which represents the findings from 40 reports GAO published in the last two years on cybersecurity.

The report emphasized the need for “significant attention” from the U.S. federal government to establish a comprehensive cybersecurity strategy and perform effective oversight. Key to this is the creation of a central role in the executive branch to implement the national strategy once it’s compiled.

Congress authorized the creation of the Office of the National Cyber Director within the Executive Office of the President to do just that. And in April, U.S. President Joe Biden nominated John Chris Inglis to fill the role. But he had not been approved by the U.S. Senate as of *Security Management’s* press time.

With the issuance of the executive order, there is an even more urgent need to fill this position as whoever holds it will be instrumental in implementing the order—as well as hiring support staff to oversee the work.

“The legislation called for several dozen positions to be created and filled within the office,” Marinis says. “To get to that point and get fully up and running will take time.... The urgency is there. We don’t have time to waste on this issue.”

Jennifer Franks, director of IT and cybersecurity issues at GAO, says that the ability to implement the numerous mandates outlined in the executive order is top of mind.

“You can establish policies and procedures, but what we do is look at the implementation strategies of what these agencies are doing,” she says. “The executive order establishes a clear timeline of what you should be accomplishing, who you should be coordinating with, and how to communicate with others what you have been accomplishing.”

Previous administrations have gotten to the point where they have organized priorities on cyber threats, but they have not been able to execute a governmentwide strategy.

“That’s been difficult,” Marinis adds. “There are many things going on across the federal government that are good, but it’s hard to know what effect they’re having until you combine them—then you could find opportunities to share lessons learned, increase the capacity of one program over another, and get a sense of urgency that is missing from a lack of clarity on who is running point.”

One crucial area that needs to be addressed is incident response to cyber intrusions, data breaches, or attacks. In 2019, the GAO found that most of the 16 agencies it reviewed had incident response processes with “key shortcomings” that limited their ability to minimize damage from attacks.

The executive order sets out to solve this problem, laying out a process to create a standardized playbook and set of definitions for cyber incident response by federal departments and agencies.

“Recent incidents have shown that within the government, the maturity level of response plans vary widely,” the White House fact sheet said. “The playbook will ensure all federal agencies meet a certain threshold and are prepared to take uniform steps to identify and mitigate a threat. The playbook will also provide the private sector with a template for its response efforts.”

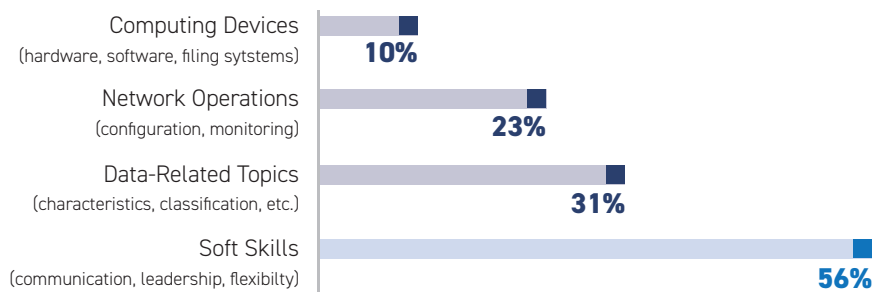
The GAO also highlighted the need for the federal government to take action to protect critical infrastructure, explaining that the government had only implemented 30 of GAO’s recommendations in this area out of nearly 80 made since 2010. This need became even more paramount the week that Biden signed his executive order, during which a ransomware attack caused a major oil and gas pipeline company, Colonial Pipeline, to shut down operations. While not an attack on federal networks, the incident that began on a private network could have cascaded to create a national security issue.

Marinis says he is encouraged to see the emphasis the executive order placed on addressing critical infrastructure security through improving mechanisms for information sharing and supply chain security. Both of these initiatives will boost the federal government’s cybersecurity while also enhancing the private sector’s security, he says.

The GAO has also made additional recommendations that need to be implemented, including that federal agencies with lead roles in protecting critical infrastructure collect and report on improvements from using the Na-

Skill Gaps

When asked, “What are the biggest skill gaps you see in today’s cybersecurity professionals?” most professionals said soft skills are lacking in the current workforce.



Source: *State of Cybersecurity 2021*, ISACA, May 2021

tional Institute of Standards and Technology (NIST) Cybersecurity Framework and more specific recommendations, such as plans developed by the U.S. Department of Energy (DOE) for electric grid cybersecurity.

“DOE had developed plans and an assessment to address the risk to the electric grid; however, we found that these documents did not fully address risks to the grid’s distribution systems,” according to the GAO report. “To address this issue, we recommended that DOE more fully address cyber risks to the grid’s distribution systems in its plans to implement the national cybersecurity strategy for the grid.”

In April 2021, the DOE announced it would begin a 100-day plan to address cybersecurity risks to the U.S. electric system.

“The United States faces a well-documented and increasing cyber threat from malicious actors seeking to disrupt the electricity Americans rely on to power our homes and businesses,” said Secretary of Energy Jennifer M. Granholm in a statement. The plan encourag-

es electric grid owners and operators to implement measures or technology to enhance detection, mitigation, and forensic capabilities related to cybersecurity. It also created milestones for owners and operators to identify and deploy systems that enable near real-time situational awareness and response capabilities in critical industrial control system and operational technology networks.

Additionally, the GAO recommended that the Federal Aviation Administration (FAA) prioritize oversight of evolving cyber threats and increasing connectivity between airplanes and other systems; that DHS update its guid-

The playbook will ensure all federal agencies meet a certain threshold and are prepared to take uniform steps to identify and mitigate a threat.

ance for the Chemical Facility Anti-Terrorism Standards (CFATS) program, such as incorporating training practices and identifying workforce cybersecurity needs; and that the Transportation Security Administration (TSA) fully incorporates NIST cybersecurity standards into select assessments for the transportation sector.

“Until our recommendations are fully implemented, federal agencies may be limited in their ability to ensure the critical infrastructures are protected from potentially harmful cybersecurity threats,” according to the report.

The executive order is a good start, but Marinos and Franks say it falls short of the national cybersecurity strategy that the United States needs.

“The reality is that without that and seeing how the executive branch will take action to implement a national comprehensive cybersecurity strategy, we will be left with questions,” Marinos says. “Are we best positioned for future attacks that are going to continue to evolve—just like the technology we rely on?” ■

**PD 6500i
PINPOINT
DETECTION**

Featuring:

Quick-Q™

When used with Garrett’s enhanced walk-through metal detectors, the Quick-Q™ technology does not require the divestment of cell phones or other small metallic items

- Quick-Q technology means we quickly speed you through the scanning process
- Crowd reduction outside of each venue
- Fewer false alarms
- Faster lines

GARRETT
METAL DETECTORS

GSA Contract Holder

garrett.com • 800.234.6151 • 1.972.494.6151

ISO 9001 CERTIFIED

Made in the USA

For product info #10 securitymgmt.hotims.com



Open

Threats are
evolving, but
are corporate
security
intelligence
methods
keeping pace?

By Mark Ashford

Illustration by Michael Austin

ON 6 JANUARY 2021,

the world watched as a large crowd of protesters violently made their way past police lines and into the U.S. Capitol building in Washington, D.C., posting videos and photos on social media throughout the riot. The night before, also in D.C., another as-of-yet unknown individual placed two pipe bombs close to the Democratic National Committee headquarters and Republican National Committee headquarters.

In April 2021, the UK's Security Service (MI5) warned that more than 10,000 UK nationals, including staff in government departments and key industries, were approached over the past five years via social networking sites by hostile state actors who sought access to sensitive information.

The common thread that ties these threats together is the candidness with which these events played out across open and public online forums and social media platforms. In completing threat assessments, we may unfairly favor confidential, closely held sources of information that appear to give us an inside track on a threat. But focusing on insider information instead of sources that are openly available to all can blind us to the obvious.

As the above examples highlight, adversaries can be very open about their intentions and objectives, often using social media or other public forums to post about future actions. Traditionally, the remit of physical security encapsulates the bounded space, employing a range of measures such as cameras, access control, perimeters, and intruder detection systems. A gap exists in managing the security of assets within the site and assessing the threats beyond it. It is not enough to produce a one-off threat assessment; there is a clear need for a more dynamic approach to identifying, assessing, and managing threats.

Part of the solution in bridging that gap to effectively ascertain and surveil threats beyond a site's perimeter is developing and incorporating open-source intelligence (OSINT) capabilities.

While OSINT began as a discipline within the intelligence community, it was quickly adopted in the cybersecurity field. However, cybersecurity professionals largely highlight aspects of the OSINT process that are most applicable to cybersecurity, such as cyber threat

intelligence. It would be a mistake to think cybersecurity OSINT is the totality of what OSINT entails.

OSINT is first and foremost an active process and thinking style. In practical terms, open-source information is the collection of publicly available information from open, freely accessible sources.

But information alone does not equate to intelligence. Intelligence is information with value added through analysis and assessment, disseminated in a timely manner to answer a key question or requirement. OSINT can include both online and offline materials—it is not a uniquely Internet-based methodology.

Threat assessments are just one part of the overall suite of security management practices for identifying and mitigating risks. Criteria for structuring threat assessments vary by virtue of the threat actor, the nature of the intersecting risk, and the type and value of the asset. However, threat assessments largely follow the core concepts of threat identification, ascertaining threat capabilities, and managing the assessed threat. The threat assessment process must become more dynamic to better manage and understand not just the threat, but the threat's evolution.

Once completed, threat assessments are at immediate risk of becoming static statements and summaries; over time, the positive effect of threat assessments as a means to inform the risk and security posture of an organization become less effective or obsolete.

While the wider political drama of the U.S. presidential elections played out over months, the activities around ideation, planning, and action leading up to the 6 January U.S. Capitol riots may have occurred over only weeks. OSINT offers the ability to shift the threat assessment from a static statement into a dynamic cyclical process—a continuous threat assessment.

There is a need to regularly and actively re-evaluate intelligence as new questions arise, assumptions are challenged, and new information comes to light. This cyclicity is what makes OSINT an active process and thinking style—not merely a “check the box” exercise. By incorporating OSINT into threat assessments, a framework can be structured

around the core aspects of the intelligence cycle—clear planning and direction, a managed collection strategy, processing information, structured analysis, and, finally, disseminating intelligence to key decision makers so they can take action.

OSINT should seek to build a profile of the areas where threat actors are active, such as forums and discussion boards, which would help map their intentions. As those sources of information inform the assessment process, they also establish the network to enable continuous monitoring and reporting, facilitating the routine updates security managers need for decision making and security posturing. The threat assessment becomes a living document, highlighting the social networks and online spaces where the threat actors are active. The result is a combined outlook of threat capabilities and a vital list of sources that can continually monitor and report information.

Determining the right places to look for such information can first appear daunting, but using the intelligence cycle will help narrow the search. Ideologically extremist groups, for example, seek to deliver their message to the public. In doing so, groups create portals between their covert operations and publicly available outlets. An adept OSINT process will help identify these portals, glean information of value, and provide intelligence input to a threat assessment.

A CLEAR DIRECTION

Incorporating OSINT into threat assessments should lead with a focused direction aided by clear planning. The quantity of data and information available will mean that without effective direction and planning, an unstructured threat assessment exercise will inevitably flounder when wading through vast volumes of information. Direction—consisting of a specific query—helps set the groundwork for an OSINT investigation, and it will affect the success or failure of the threat assessment exercise.

The query should be realistic and practical. The direction should not attempt to steer the

OSINT investigation to predicting the unpredictable or quantifying the obvious—for instance “when will the next pandemic occur,” or “will there be a terrorist attack in Europe within the year.” Taking the latter, given the breadth of terrorism risks within Europe, a terrorist attack within the year is a near certain occurrence. Pursuing these thought exercises does not help inform how we manage the risk, likely timescales, or types of attack.

Specificity is key to relating the threat to an organization, while also having the added benefit of focusing the search parameters of the OSINT stream. For example, terrorism is too wide a threat—narrow the focus down to a particular terrorist group, modus operandi, or location. Framing the wider understanding with focus on the specifics of the threat will add value to the outcome of an OSINT assessment in terms of turnaround time and resource management. Multinational organizations, for example, cannot rely on a threat assessment that seeks to capture a terrorist group’s global ambitions or lists the number of attacks.

OSINT planning calls for breaking down the key information required into more manageable parts. Exercises in probabilistic thinking will help manage the OSINT threat assessment into its key parts. Probabilistic thinking can be both a quantitative or qualitative practice and seeks to identify the most likely outcome from an event among multiple likelihoods. It is the act of building up sources of information and knowledge around possible outcomes to try and reduce the element of uncertainty as much as possible.

Planning a threat assessment around OSINT methods should initially quantify what is known, what can be learned, and the unknowable, while teasing out any biases, all of which will affect the threat assessment outcome.

Biases are an inherent part of assessments. They can lead to the wrong conclusions, so the information, our views, and our statements should constantly be challenged to identify what is actually important. There are many identified knowledge biases, such as anchoring and availability biases, which place an over-reliance or over-emphasis on the first available piece of information or drive assessments based on the immediate information to hand. The speed of new information generated online and the resource demands on physical security departments underline how OSINT investigations are made in a

continuously volatile and dynamic environment—both online and outside of the Internet. Planning will significantly signpost the areas where you need more information and where you need less, mitigating the risk of interference from bias. Additionally, probabilistic thinking in the planning stage will help navigate the problems of accuracy in dealing with inherently unreliable information—whether that’s social media, disinformation, or deliberate obfuscation.

COLLECTION STRATEGY

The next stage is to establish the collection strategy, the value of which will be built off of earlier work during the direction and planning stages. There has been significant growth in commercial OSINT gathering platforms and products in recent years—a trend that is likely to continue. From forensic browser software to continuous geo-fencing for social media triggers to commercial satellite imagery, there is most likely a commercial collections platform catering for your specific security needs.

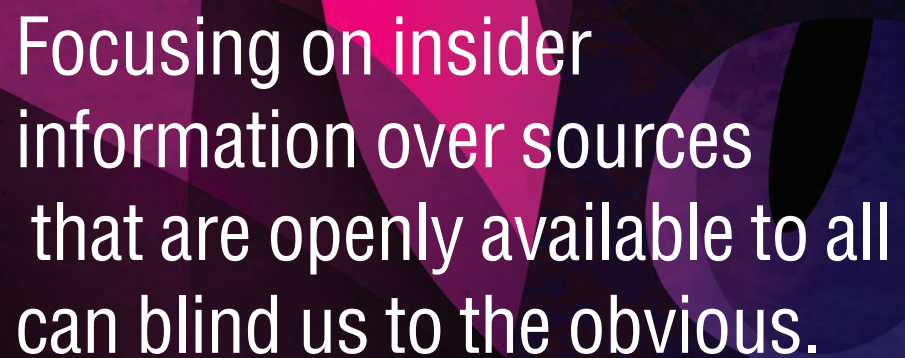
Myriad areas will govern the type and extent of the OSINT collection strategy. Some will be practical considerations—how many team members are free to spend time collecting information or what technical resources are in place to enable both information collection and routine security responsibilities. Accurate planning of OSINT and threat assessment requirements up to this point

should ensure that the capabilities and demands are as evenly matched as possible. For instance, would the general media and public relations information from a threat group sufficiently answer key threat assessment questions, or is there a need to be involved in an online forum actively used by members of that same group? Understanding where additional effort is required can help identify efficiencies.

Additionally, there are clear safety, security, and organizational considerations to address long before executing information-gathering activities. A collection strategy should account for any deterrents—legal, financial, or reputational—that may impede the work. Risk appetites, ethics, and moral considerations all play a part in determining appropriate OSINT activities. Consider the 2018 Cambridge Analytica scandal, in which a political firm harvested tens of millions of users’ personal data from Facebook. Although the action was legal, it had long-term reputational and data privacy implications.

Flexibility is important. As part of the organization’s security practices, threat assessments might only be an annual exercise. Like with the U.S. Capitol riots, however, the subject of the threat assessment could change weekly, and the security response will depend on the level of information secured from the collections plan, which may need to change to keep up. Building in flexibility enables adaptability.

Threat assessments can be subjective exercises, and there may be additional signals within the collected information that signify



Focusing on insider information over sources that are openly available to all can blind us to the obvious.

a change in interpretation is required. Consider how rapidly social justice movements and protests spread worldwide—massive social unrest can start from subtle events half a world away, triggering local tensions and sparking disruption. Events do not happen in isolation, and everyday ordinary signals can come to mark the start of world events. With the information we collect, we should be constantly looking to see how even the small pieces could impact our understanding.

Online entities, including social media, are making personal and professional information freely available on a massive scale, providing real-time access to imagery of localities, records of local events, as well as details of subjects' social and professional contacts. The value of such information cannot be overstated. Online and offline social engineering attacks are built upon the freely available, in-depth personally identifiable information (PII) that exists across numerous platforms, including social media.

An OSINT collection strategy will inevitably touch upon PII, and—depending on

for commercial or private security management work. As such, if you, your organization, or the subject of an OSINT investigation resides in the EU, investigators will likely have to reckon with the GDPR. Additionally, the GDPR equally applies to the processing of personal data online or offline, whether in social media, employment, or government records.

Under the GDPR, an OSINT investigation will likely need a legal basis for processing PII, and it should apply certain principles on how it is processed, such as data security, accountability, and governance, as well as identifying and incorporating the subject's rights. Compliance requirements, from GDPR to an organization's capacity for data storage, underline how available resources will be a key consideration.

One of the most frequent asks from OSINT, even by other OSINT practitioners, is the need for a list of tools, as though such a list will lead to direct success. It should come as no real surprise that there is no one OSINT program list or resource that will do it all. Rath-

PROCESS AND ANALYSIS

Given the wide variability in types of information and concerns over its reliability and credibility, processing is an integral element to OSINT.

Where the required information is amenable to primary and secondary sources, look to reach for the former: direct eyewitness evidence is worth more than third- or fourth-hand information, and we should grade the information as such. Where threat assessments necessitate OSINT investigations into more uncertain areas, such neat classification of sources may not always be readily available. As such, OSINT investigators should consider the Admiralty or NATO System to help evaluate the collected information.

Under the Admiralty System, information is judged on reliability—based on the source's past reporting, whether there are doubts about its authenticity or trustworthiness, and the competency of the source. Information judged on reliability is graded A through F. Credibility is assessed against whether the information can be corroborated against other sources or against what is already known about the matter. Credibility is graded with a numerical value between 1 and 6.

If an eyewitness to a popular event provides direct, first-hand information that can be checked against other sources, for example, that source would be graded A1. A person reporting information that they have overheard but have no direct experience of—and they are reporting for the first time—would likely be graded F6.

The purpose is to build confidence in the accuracy and reliability of gathered information by using the different grades to add nuance and context to pieces of information and better inform decisions.

There is an inherent risk in any method of information collection to always want more—more time or information with which to make decisions. A fatal risk for the OSINT threat assessment can materialize by coming to a conclusion too early or failing to come to any meaningful conclusion at all. Information collected, processed, and analyzed via OSINT methods will invariably change, and it will never remain static. An OSINT-led threat assessment inherently enables dynamic monitoring over a static statement of intent.



It would be a mistake to think cybersecurity OSINT is the totality of what OSINT entails.

the legal frameworks you are operating under—organizations will need to consider how such information is identified, recorded, and stored.

The European Union's General Data Protection Regulation (GDPR) is a wide-reaching and wide-encompassing document governing PII and its use. Exemptions exist for OSINT activity as it pertains to national security and law enforcement (which have separate directives). However, there is no specific or general exemption under GDPR

er, OSINT practitioners will usually build up personal knowledge of tools, useful sites, and a network of OSINT practitioners that fit their specific needs. When deciding what collection methods and tools to use, overriding consideration should always be given to safe security practices, while keeping in mind the legal, personal, moral, and ethical implications of engaging in OSINT collections methods. The adverse legal implications may apply equally to the OSINT analyst and the organization.

DELIVERY

The final component is the delivery of timely, relevant, and actionable findings to key decision makers, be they within the physical security remit or wider executive leadership positions. Invariably, there are in-house writing style requirements, but they should not impede conveying the key judgments and important information effectively to a reader who may not have time to read an entire assessment in detail.

Ideally, the assessment should be written for the person or department that requires

it. For instance, undertaking a threat assessment for a member of staff traveling overseas may simply require a cover page with the key findings for his or her manager while the body of the assessment remains within the relevant security department. In other cases, a threat assessment may be forwarded to an internal investigation department or a wider audience, in which case the assessor may seek to withhold certain aspects or findings until later. A formulaic process will fail.

OSINT is an evolving framework, ideally suited to dynamically assessing evolving threats. The challenge of unreliable information, especially in today's age of disinfor-

mation, is not insurmountable. Additional issues remain, such as managing people's expectations of the OSINT process, the requirements for training and technology, and resource allocation. However, employing the intelligence cycle as part of the threat assessment process will help make the most of resources at hand within the time available. ■

Mark Ashford works in security risk analysis and threat assessment in the financial industry, following a 12-year background in law enforcement and state security. His other areas of interest include intelligence analysis, strategic foresight, and international relations.

CONVERGED INTELLIGENCE SOURCES

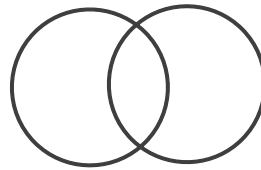
OSINT is not a wholly Internet-based intelligence process. Information can come from offline, online, or blended sources.

OFFLINE SOURCES



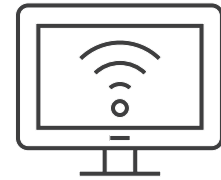
- Company record searches
- Patent and trademark offices
- Real estate companies
- Speaking events (talks and presentations)
- Government publications
- Offices and universities (grey literature)
- Radio
- Television

BLENDED SOURCES



- Government agencies
- News media
- Political leaflets and manifestos
- Birth, death, and marriage certificates
- Criminal and court proceedings
- Local planning applications
- Land registry and home ownership records
- Academic research
- Charities or non-governmental organizations

ONLINE SOURCES



- Social media platforms
- Online blogs and forums
- Think-tank websites
- International agencies
- Online map and surveillance providers
- Reverse imagery checks
- Dating apps
- Dark Web
- Online domains and metadata databases
- Video and file sharing sites

PROFITING OFF THE



NEW ABNORMAL

DURING A PANDEMIC, THE
THREAT OF ORGANIZED
CRIMINAL ACTIVITY
EVOLVED TO SURVIVE AND
TAKE ADVANTAGE OF NEW
BUSINESS OPPORTUNITIES.

BY MEGAN GATES



IT STARTED

the way an investigation into an organized crime group often does. Investigators identified a group of Colombian, Dominican, and Spanish nationals who were part of a large-scale cocaine, hashish, and marijuana trafficking operation out of Cataluña, Spain. The authorities seized several shipments of cocaine in Colombia that were linked to the group—approximately 2,900 kilos worth.

But then, things took a turn. In February 2021, authorities arrested four individuals connected with the group in Tarragona, Spain, and seized 583 kilos of hashish that was intended for France and Italy. During the subsequent search of a warehouse used by the group, the authorities found half a submarine.

“The boat—the first ever of its kind seized on European soil, was still in construction when it was found,” according to Europol. “The craft was 9 meters long and could have been able to transport up to 2 tonnes of drugs.”

More than 300 police officers were involved in the operation, with support from the National Police of Colombia, the Dutch National Police, the Portuguese Judicial Police, the UK National Crime Agency, and the U.S. Customs and Border Protection Agency, with additional coordination aided by Europol.

The submarine, which the criminals presumably built to enhance their drug transportation capability, shows the lengths organized crime groups will go to in 2021 to evade detection and extend their reach during the COVID-19 pandemic—a time of economic turmoil with an element of global chaos.

In its most recent *Serious and Organised Crime Threat Assessment (SOCTA)*, published in April 2021, Europol found that nearly 40 percent of the criminal networks active in the European Union are involved in the trade of illegal drugs, roughly 60 percent of these networks use violence as part of their criminal businesses, and that more than 80 percent of the criminal networks use legal business structures to facilitate their operations.

“The analysis indicates that criminal structures are more fluid and flexible than previously thought, use of violence by organized crime appears to be increasing, and use of corruption and abuse of legal business structures are key features of serious and organized crime activities,” wrote Europol Executive Director Catherine De Bolle in the report.

Europol’s analysis found that organized crime in 2021 is more flexible and changing in nature, “connecting individual criminal entrepreneurs and smaller groups of criminals mediated by information and contract brokers and supported by criminal service providers lending advice and assistance with expertise in law, finance, logistics, and many other specialist domains.”

The COVID-19 pandemic has also had a significant impact on the organized crime threat landscape in Europe, reshaping how criminal networks operate and uncovering new opportunities for them to thrive on.

“I am concerned by the impact of serious and organized crime on the daily lives of Europeans, and growth of our economy, and the strength and resilience of our state institutions,” De Bolle explained. “I am also concerned by the potential of these phenomena to undermine the rule of law.”



Terrorism and serious and organized crime continue to pose the “most pressing internal security challenge” to the European Union, according to the 2021 *SOCTA*. This criminal activity ranges from the illegal drug trade to migrant smuggling to human trafficking to economic and financial crime.

“The trade in cocaine, cannabis, synthetic drugs, and new psychoactive substances is a key threat to the EU due to the levels of violence associated, the multibillion-euro profits generated, and the substantial harm caused by it,” the *SOCTA* explained.

Of the groups behind these practices, one in four has been active for more than 10 years; 40 percent use a hierarchical structure, compared to 60 percent with a fluid crime structure; and 79 percent have six or more members. Europol’s analysis found that more than 180 nationalities are involved, with seven out of 10 groups active in more than three countries.

“More than 50 percent of all reported suspected organized criminals active in the EU are non-EU nationals,” the *SOCTA* said. “Half of these non-EU nationals originate from countries in the EU’s neighborhood, such as the Western Balkan region, eastern European countries, and North Africa.”

A concerning trend highlighted in the report is that the level and use of violence associated with organized crime increased in frequency and severity since 2017.

“Violence in illicit markets is often a sign of growing competition (e.g., over the control of lucrative distribution networks or a particular geographic territory),” according to the *SOCTA*. “Shifting power balances within or between competing organized crime groups, the impact of law enforcement efforts, or broader economic pressures can also generate violence.”

This violence is seen in the form of threats, intimidation, vandalism, assault, kidnapping, torture, mutilation, and murder. It also takes the form of internal violence—within the group itself—to settle conflicts or punish individuals for breaking the group’s rules.

One of the major economic pressures that organized crime faced in 2020 and into 2021 was the threat of economic decline or recession related to the COVID-19 pandemic. In some instances, organized crime was able to take advantage of the situation.

“Criminals were quick to adapt illegal products, *modi operandi*, and narratives in order to exploit the fear and anxieties of Europeans and to capitalize on the scarcity of some vital goods during the pandemic,” according to the *SOCTA*. “While some criminal activities will or have returned to their pre-pandemic state, others will be fundamentally changed by the COVID-19 pandemic.”

In an analysis for Corporate Compliance Insights, Stefano Siggia, senior consultant at Pideeco, explained that the pandemic allowed mafia groups—such as the Sicilian Cosa Nostra, the Neapolitan Camorra, the Apulian Sacra Corona Unita, and the Calabrian ‘Ndrangheta—to acquire bankrupted entities and use them for profit, especially in Italy where COVID-19 hit particularly hard.

During 2020, banks lent less money to small- and medium-sized businesses, and the government saw an increase in requests for food aid from charities. In response, mafia groups took to distributing food to families facing financial difficulties—possibly as a recruitment method for business deals—and mafia organizations acquired failing businesses to help them obtain short-term financing in exchange for laundering money.

This also tied into another major finding from the 2021 *SOCTA*, which found that criminal networks are increasingly using legitimate business structures to enable their activities, such as through money laundering to integrate illicit funds into the legal economy.

“The COVID-19 pandemic may be followed by an economic recession,” the report said. “It is likely that criminals will exploit vulnerabilities in the economy to infiltrate legal businesses in order to facilitate their criminal activities. This may entail loaning funds to struggling businesses and making them dependent on criminal financiers or directly buying up companies in financial difficulties.”



SOUTHEAST ASIA

Halfway around the world in Indonesia, the COVID-19 pandemic is also having a major impact on organized crime. In normal times, millions of tourists flock to the country—and its famous island of Bali—but with the pandemic and subsequent travel restrictions, tourism spending was drastically down in the nation.

That’s when Adam Darrah, director of intelligence at Vigilante, and his team began noticing some odd online behavior. Due possibly to economic desperation, more individuals in Indonesia were turning to the Dark Web to buy access to stolen credentials, including those for bank accounts and streaming services like Netflix.

Before COVID-19, most cybercrime activity out of Indonesia centered around cyber activism in the form of website defacements, Darrah says. “They didn’t have a high reputation in the cyber criminal underground like the Chinese or the Russians,” he adds.

After COVID-19, more entry-level actors started engaging online with higher profile actors, asking for help to buy tools to use for cybercrime.

“We’re seeing an influx of requests for help: Where do we go to buy stuff? How do we buy stuff? Or do you know anyone who can help us increase our followers, say on Alibaba?” Darrah explains.

While some of these requests for help are happening on the Dark Web, some of them are being facilitated through one of the more obvious channels: Facebook. Darrah says Vigilante has seen an uptick in advertisements from criminal groups on Facebook, using the site’s

advertising features to reach an audience that is then directed to testimonials and group chats on WhatsApp—also owned by Facebook.

In 2019, Facebook announced it removed hundreds of Indonesian accounts, pages, and groups, after discovering they were linked to an online group engaged in spreading fake news and hate speech.

“These accounts and pages were actively working to conceal what they were doing and were linked to the Saracen Group, an online syndicate in Indonesia,” said Nathaniel Gleicher, Facebook head of cybersecurity policy, in a statement.

However, as of *Security Management*’s press deadline Facebook had not taken action on the activity identified by Vigilante. And the ability for these criminals to learn, network, and market services on social media and online highlights another cause of concern for investigators looking to tackle organized crime—their increasing ability to use the Internet for gain.

**I AM CONCERNED BY THE IMPACT
OF SERIOUS AND ORGANIZED CRIME
ON THE DAILY LIVES OF EUROPEANS.**

“Social media mirror advertisements on websites and serve as dedicated channels for marketing or communication channels for criminal networks,” the *SOCTA* found. “All available illicit goods and services are also visible on social media.”

Europol also noted that organized criminals may use disinformation campaigns to generate sales for their products or lure individuals into fraud schemes. In addition, the law enforcement organization warned about a rise in the trend Vigilante had noticed in Indonesia—cyber-crime-as-a-service.

“Criminal tools such as malware, ransomware, phishing facilitators, sniffers, skimmers, and distributed denial-of-service attacks are offered online, especially on the Dark Web,” the *SOCTA* said. “The crime-as-a-service business model makes criminal services easily available to anyone, lowering the level of expertise previously required to perform specific criminal activities.”



AFRICA

Just as the world has become increasingly digital and mobile, so too has currency and banking. Nowhere else is that more apparent in the world than in Africa, which is considered the world leader in the mobile money industry with more than half of all registered mobile money accounts globally, according to Interpol.

Mobile money is generally a service that people can use to store, send, and receive money by using a mobile phone instead of a traditional brick-and-mortar bank. Users can also withdraw cash from authorized agents associated with their mobile money provider.

The ability to pay using only a mobile phone has aided the growth of Africa's economy, but it also provided opportunities for organized crime groups to take advantage of the service.

In a 2020 assessment, Interpol found that the “lack of robust identity checks to verify users combined with a need for greater law enforcement resources and training on mobile money-enabled crimes have created a financial system distinctly vulnerable to criminal infiltration.”

Interpol said there were “strong indications” that mobile money is enabling criminality and poses a “significant threat” to African society through its use for terrorism financing, money laundering, extortion payments, human trafficking, people smuggling, and the illegal wildlife trade.

“In addition to this, mobile money service exploitation by criminals benefits from poorly applied regulations and expertise in the criminal justice system,” Interpol explained. “If this is not addressed, there is a significant risk of further criminal proliferation due to perceived risks versus rewards.”

This is especially concerning because the Global System for Mobile Communications Association (GSMA), which represents the interests of more than 750 mobile operators and 400 companies, said the mobile money market grew exponentially during the COVID-19 pandemic in response to lockdown restrictions.

GSMA's annual *State of the Industry Report on Mobile Money*, published March 2021, noted that the “number of registered [mobile money] accounts grew by 13 percent globally in 2020 to more than 1.2 billion—

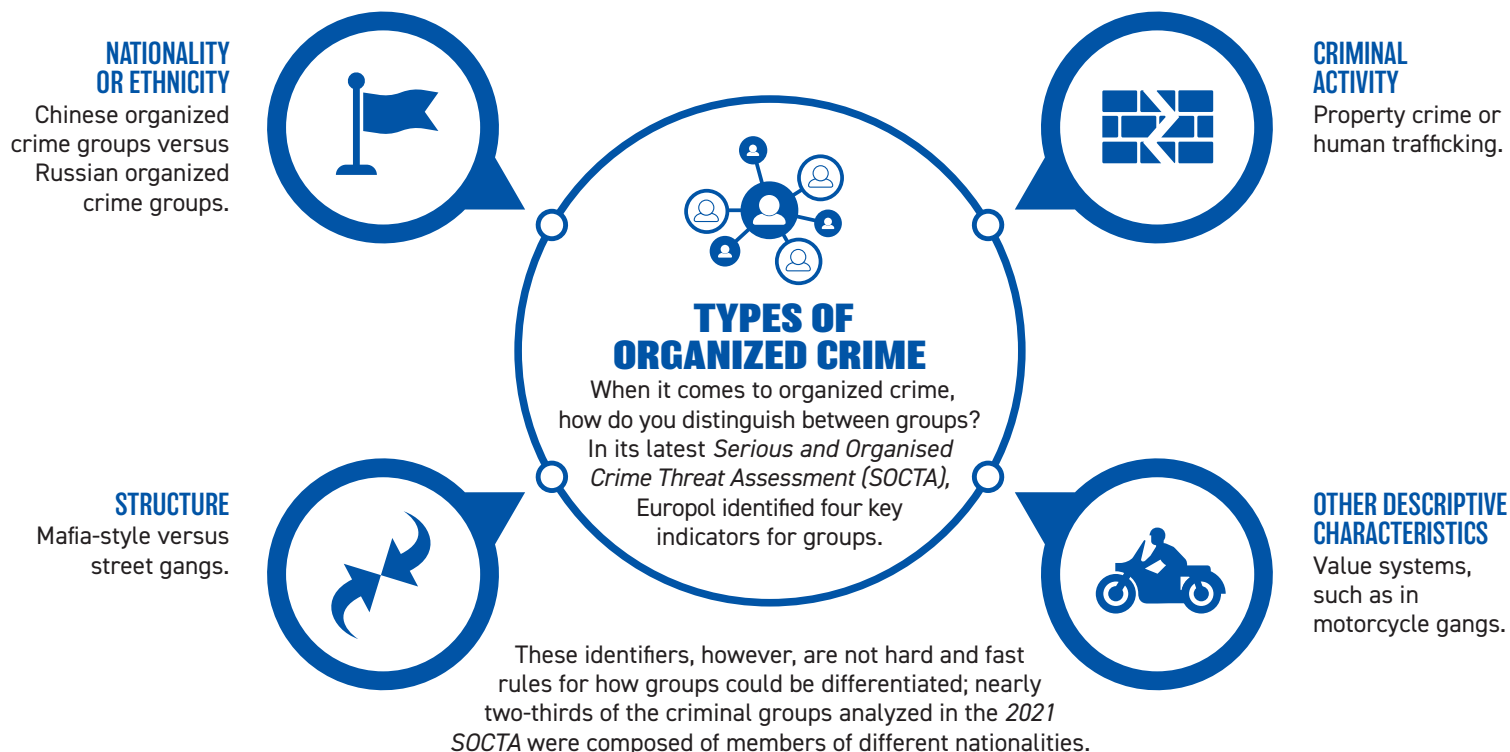
VIOLENCE IN ILLICIT MARKETS IS OFTEN A SIGN OF GROWING COMPETITION.

double the forecast,” with the fastest growth happening in markets where governments provided relief to their citizens.

Additionally, in response to COVID-19 restrictions, some governments made regulatory changes to better facilitate mobile money payments, such as classifying them as essential services and increasing transaction limits to allow more funds to be transferred at one time.

Along with using mobile money markets, organized crime groups in Eastern Africa are taking advantage of the COVID-19 pandemic to move into the illicit medications market.

“A COVID-19 related hysteria has maximized profits for organized crime in this field, whilst enabling relatively risk-free activity for crim-



“In some cases, classifying criminal networks according to national or even ethnic homogeneity can be relevant for an investigation because the nationality and/or ethnicity can be an important element in international collaboration,” Europol said. “Strategically, the division of criminal groups according to ethnic homogeneity often lacks nuance.”

inals,” according to an Interpol assessment. “This activity has included increased importations of counterfeit and substandard medications from Asia, as well as the acquisition of powerful painkillers to sell on the black market.”

In an analysis published in December 2020, Interpol said that organized crime groups are “capitalizing” on the increased demand for medication during the pandemic, importing illicit medications through the Mombasa port because of reduced capacity to inspect incoming shipments. Misinformation is also playing a role as it spreads across social media; Interpol explained that misinformation about COVID-19 has likely “increased the general willingness to source medications via illicit means.”



LATIN AMERICA

In Latin America, the COVID-19 pandemic is impacting organized crime and the illegal drug market—especially supply, production, and trafficking chains—as many nations imposed border restrictions to limit the spread of the disease.

In a Wilson Center analysis published in October 2020, experts found that restrictions imposed by the United States—the final destination for most of Mexico’s methamphetamines, heroin, and cocaine—made it increasingly difficult for cartels to move drugs across the border. At the same time, Asian governments limited the transportation of merchandise—cutting down on the chemicals sent to Mexico used in the production of these drugs. China only recently eased some of its restrictions, allowing more shipments to Mexico.

“Thus, while the northern border still faces restrictions and interdiction measures, the local capacity for producing and manufacturing different types of illegal drugs has gradually recovered,” according to the Wilson Center report, *Social Programs and Organized Crime in Mexico*. “This situation clearly gives Mexican cartels an unprecedented and extremely delicate and risky alternative for Mexico’s national and public safety: growing, broadening, deepening, and developing the Mexican market for illegal drugs.”

To adapt to the situation, the cartels are ramping up their local capabilities and strategies for the drug market. They are also considering new avenues of funding, including providing basic goods to vulnerable populations where the government response to the pandemic has been “weak, scarce, or altogether nonexistent,” the report said.

The Mexican federal government also shifted its approach to organized crime, focusing more on the social causes of crime and violence instead of openly fighting the cartels.

“Facing less government pressure, the most powerful Mexican cartels have reinforced their distinct process of centralization and domination of territory, criminal markets, supply chain links, transportation routes, crime groups, organizations, and structures,” according to the report.

Latin America also saw an increase in violence during the COVID-19 pandemic as organized crime groups fought over territory, wrote Robert Muggah, principal at SecDev group, for *Foreign Policy*.

“Brazil’s three-year decline in homicide has come to a screeching halt,” he wrote. “In São Paulo, home to one of Latin America’s most powerful drug trafficking organizations, murders were up 10 percent between March 2019 and March 2020. And in the northern state of Ceará, violent crimes (including homicide) spiked by 98 percent in just 10 days in March. Levels of reported domestic violence have also surged in most states, including by more than 50 percent in Rio de Janeiro alone.”

Muggah tracked similar levels of rising violence in El Salvador, finding that mafia, militia, and criminal groups were reinforcing their soft power in the regions where they operate.

“In addition to fueling rising violence, the pandemic could enhance the social, economic, and political clout of some criminal organizations in the same way that the Italian mafia and Japanese yakuza emerged stronger after the great dislocations of World War II,” he wrote. “Crime bosses know full well that law enforcement and criminal justice systems are overstretched and that prisons are bursting at the seams in Latin America and elsewhere. They also know great scarcity is coming, which may increase the risk of violence. The question is whether we are even remotely ready.” ■

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



GET A MASTERS DEGREE IN SECURITY MANAGEMENT IN 18 MONTHS.

- **BS/MS in Security Management**
- **MS in Emergency Management**

**JOHN
JAY**
COLLEGE
OF CRIMINAL
JUSTICE
ONLINE

CUNY

ENJOY IN-STATE TUITION PRICING NO MATTER WHERE YOU LIVE.

Visit JohnJayOnline.com

For product info #11 securitymgmt.hotims.com

By Claire Meyer

A TWO-WAY STREET

COVID-19 has wreaked havoc on global workforces. To retain and foster future leaders amid the tumult, personal connection through mentorship can provide support and grow both mentor and mentee.



While 76 percent of people consider mentors important, only 37 percent actually have one, according to a 2019 Olivet Nazarene University survey of 3,000 full-time employees in the United States. Most mentoring relationships developed naturally, with nearly 40 percent of mentorship relationships beginning with a request or offer, the study found. But therein lies the gap—without proactive action, mentorships are unlikely to get off the ground.

Mentorships offer an opportunity to surmount another prescient workplace dilemma: cross-generational conflict and management. Management books and Internet articles abound with complaints and potential solutions about how Baby Boomers (born 1946–1964) could work with Millennials (born 1981–1996) or how Gen X (born 1965–1980) could steer the work culture of Gen Z (beginning 1997)—the latest generation of politically active, digital-native employees entering the workforce. And while there are many sticking points between generational norms, personal relationships through mentoring can help individuals connect more seamlessly across the workforce—especially in a field with as much professional longevity as security.

“The security field is unique; it seems we never really retire, as this is more of a profession and calling than a job,” says Jennifer Hesterman, security consultant, author, lecturer, and a retired U.S. Air Force colonel. “As a result, there are four generations now represented in our workforce, with an age span of 55 years from new security professionals to the most seasoned. Although many see this as a challenge, it provides an incredible opportunity to tap vast knowledge, broad experiences, and a variety of technical and soft skill sets.”

“Mentoring is a powerful tool in leadership development, as it transfers knowledge and skills to the next generation of leaders,” she adds. “We don’t want to get into a position down the road where we lack a robust pool of people to lead the security industry. Academia is facing this very challenge and hiring college presi-

dents from the business sector, the military, and other realms. Not that an outside perspective isn’t refreshing and welcome, but mentoring efforts can help us build a large pool of tested, prepared, and willing security leaders for the many challenges on the horizon.”

And that pipeline of capable and diverse leaders is needed. The tumult of the COVID-19 pandemic continues to shake up workforce demographics. Globally, women make up almost two-fifths of the global labor force, but they have suffered more than half of total job losses from the pandemic, according to the World Economic Forum.

In the United States, McKinsey & Company research found that one in four women are considering leaving the workforce or downshifting their careers due to the pandemic, compared to one in five men. Three major groups experienced some of the largest challenges: working mothers, women in senior management positions, and Black women. They were driven to the brink of dire career decisions by a variety of factors, including the stress of juggling home and work responsibilities while trying to meet pre-pandemic performance goals, feeling blindsided by decisions that affect day-to-day work, and difficulty talking with coworkers or managers about the challenges they face.

“There are so many factors that will change our demographics due to COVID,” says Donna Kobzaruk, executive director of global security for financial services company JPMorgan Chase. “It’s indisputable that women have left the workplace in droves. Women have made strides in diversity numbers only to see it’s changed. That’s why it’s even more imperative for women, as well as young professionals, to seek out a mentor. A mentor can guide you in having a voice and raising your profile within an organization.”

Different age groups have also been affected by the pandemic. A 2021 report from the National Council on Compensation Insurance found that U.S. workers between the ages of 16–24 experienced a 30 percent decline in employment, while older workers are on the rise with an expected 50 percent growth in U.S. workers over the age of 65 in the next decade. This will likely widen the age range in the security industry.

A multigenerational workforce, however, can offer opportunities—as well as challenges. Shelly Kozacek, CPP, director of security for ship repair at aerospace company BAE Systems, has been managing employees spanning the generational spectrum throughout four U.S. sites for years.

It is exciting for her “to have someone from generation Baby Boomer or Generation X to team up and mentor someone from Generation Y or a new college graduate,” she says. “There is a lot to be learned on both sides... The mentorship relationship is so valuable because both people learn from the experience. Getting that insight from someone you might not team up with yourself is really helpful.”



Mentoring efforts can help us build a large pool of tested, prepared, and willing security leaders for the many challenges on the horizon.

Over her 20-year career so far, Kozacek was first mentored by a knowledgeable and personable supervisor 30 years her senior who stepped forward to share his skill sets and leadership approaches while Kozacek served in the U.S. government. This mentor later became a peer she could lean on to determine what her role entailed and how she could expand her value when helping clients and the organization. Later in her career, Kozacek became a mentor, including through ASIS International, gaining as much value as she imparted, especially when it comes to her mentee's technical skill set and digital savvy.

"Initially, in a mentorship, what you gravitate towards is trying to learn about daily ins and outs of certain processes and procedures, especially if they are internal to your organization, and trying to navigate past experiences," she says. "My experience has been—in a mentorship relationship—once you're beyond that initial 'learning the ropes of the job' stage, the mentorship relationship flourishes into more of an understanding of the leadership and how to reach—how to obtain that next level."

Different generations and career stages have different mentorship needs, adds Kobzaruk, and mentor-led guidance can often focus on subjects that mentees cannot learn in a class or a book. Someone new to the security profession may need to focus on soft skills and cultural knowledge of the industry and his or her organization. A mid-level employee may need to focus on leadership skills, and once he or she has a firm grasp of the basics, the individual may need help learning how to progress up the hierarchy. Senior executives and leaders may also benefit from being co-mentored by a peer or a counterpart at a different organization or department to share management approaches and problem-solve.

"One of the more difficult items to grasp is organizational cultures," Kobzaruk says. "When was the last time you've seen a class on knowing your organization's culture? Having this knowledge will support a future leader on his or her trajectory into a leadership role, and a mentoring relationship is invaluable with maneuvering through cultures."

Mentees should seek out mentors with savvy in the skills they want to learn, Kobzaruk advises.

"If a mentee would like to strengthen his or her leadership skills, look for a mentor that's a well-respected leader in the industry," she says. "The leader may be one level above or several."

From her experience in the military, Hesterman says she finds that mentoring programs centered around a formal chain of command often fail. "Forced mentoring is uncomfortable for both mentor and mentee," she says. "A mentor is someone we naturally gravitate towards."

Sacrificing family, friends, outside interests, and personal health for work is not acceptable to new generations entering the workplace, nor should it be.

This might shift mentoring relationships outside typical manager–employee relationships, which is not necessarily a bad thing. Hesterman adds that bosses can be seen as coaches—people who are concerned with employees' professional development—while mentors have a more holistic view of the mentee's growth as a human.

"If the goal is to climb a mountain, a coach will provide fitness, nutrition, and equipment guidance—helping with the 'how,'" she says. "A mentor would focus on why you want to climb the mountain and help with expectation management. Both are necessary to get to the top."

Not every emerging security professional knows which mountain they want to climb, however. Author Lewis Carroll once said, "If you don't know where you are going, any road will get you there."

Professionals who are seeking to climb the ladder but can't quite find the first rung need some help, says Danny Chan, senior consultant for security monitoring and response in the Asia Pacific and Middle East region for Mastercard International. Chan says he spent a great part of his career as a rudderless boat, finding out the hard way what works and what doesn't, and determining his career goals as he went along.

"As learning from someone else's mistakes is a great way to learn, I have been helping the next generation of security leaders to not make these mistakes and, more importantly, help them craft out a path towards their goals," he explains.

In Hesterman's mentoring work with college students and young adults, she says she found that "many want information on how to achieve balance between their professional and personal lives. Sacrificing family, friends, outside interests, and personal health for work is not acceptable to new generations entering the workplace, nor should it be. Employees who achieve a work–life balance experience less stress, have lower risk of burnout, and a greater sense of wellbeing. This



Mentor Matchmaking

Mentoring programs have a long history within ASIS International. The Professional Development Community and ASIS have been working during the past decade to connect up-and-coming security professionals with mentors from across the industry to foster their skills and boost their leadership potential.

The latest iteration of the program—the Security Leaders Mentoring Program—is open to all ASIS members at any job level to connect security professionals with resources, advice, and guidance. The new program features a database of mentors and mentees, so mentors can list skills and expertise and mentees can find a mentor who aligns with their objectives.

“We’re looking to increase awareness and increase use of the mentorship program as a tool for individuals to have someone to reach out to, to ask questions, and to have discussions—someone who can help you get to the next level you want to be at,” says Shelly Kozacek, CPP, director of security for ship repair at BAE Systems and a member of the ASIS Professional Development Steering Committee.

Users of the program set up a profile and can search the directory for potential mentor matches to connect with. Mentorship relationships are encouraged to run at least six months, and ASIS provides resources and handbooks to help guide new mentors and mentees.

In addition to the value of connecting with higher level professionals, both mentors and mentees can reap benefits from learning from a third party outside their own organization or sector. When feedback and guidance is completely internal to an organization, it can produce a narrower mind-set, Kozacek says. But connecting with an outside professional helps participants branch out, bounce ideas off a new person, get objective feedback, and learn from new perspectives. This also enables mentors and mentees to bring those outside lessons learned back to the organization—advancing security, as well as their careers.

The program is now accepting both mentors and mentees. Learn more at asisonline.org/mentoring.

not only benefits employees, but also employers. Take care of the people, and they will take care of the mission.”

Mentees should be willing to adjust if needed, and so should mentors. “A mentor owes it to a mentee to provide the best service he or she can,” Kobzaruk says. This means tailoring mentoring styles and topics to the individual.

“I mentored an individual who was of a different culture than mine,” she says. “Although she initially stated she wanted help in leadership skills, it became apparent that she would be better served in strengthening her communication style. When I mentioned this, it was an ‘a-ha’ moment to my mentee, and I was pleased to see her successfully use the tips I provided.”

“We should style our mentorship by providing a more bespoke approach,” Chan says. “Regardless of age, gender, or professional status, to build rapport we need to better understand someone’s personality and character. For example, are they detailed or big picture? What is their moral compass? Are they people- or system-focused?”

Knowing these elements will help a mentor to adjust and provide effective guidance that reaches the unique mentee, rather than applying a one-size-fits-all approach.

As the parent of a 23-year-old, Hesterman adds, she understands firsthand the difficulties in launching a new career. Personal insights like these help her connect to younger employees and tap into their frustrations and concerns.

“Mentoring has a direct impact on employee retention for two reasons: First, mentees appreciate the investment of time and energy in their career and personal development, feeling more closely tied to and valued by the organization,” Hesterman says. “Also, mentoring is a way for leaders to gather information—by understanding the needs of young employees, it is possible to tailor programs to meet these needs and retain talent.”

The two-way street of mentorship has proved particularly valuable around soft skills, Kobzaruk says. While she can help educate mentees about critical communications skills in the workplace, mentees can provide insights on what motivates younger generations or how to communicate more effectively with a wide audience, which provides security value—not just leadership experience.

“Communication is a critical component in the workplace, but more so in security,” Kobzaruk says. “A lot of what we do is managing anxiety. A strong communication toolkit that provides different communication styles is invaluable.” ■

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

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

Providing 1 Million Meals!



 **FEEDING**TM
AMERICA

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



Supporting Families Across America

MISSION **500**

BALLPARK FIGURES

BASEBALL STADIUMS STRIVE TO ADAPT THEIR SECURITY POSTURES AND WORK WITH THEIR COMMUNITIES TO KEEP FANS, PLAYERS, AND OTHERS SAFE, EVEN WHEN IT'S NOT GAME TIME.

By Sara Mosqueda

◆ CITIZENS BANK ◆



◆ ROGERS CENTRE ◆



◆ BUSCH STADIUM ◆



Take me out to the ballgame

As the song says, when you go out to the ballpark you're hoping for peanuts, Cracker Jacks, and a win for your home team. The game attracts all, regardless of background, ethnicity, sex, creed, or fame. Actor Humphrey Bogart was so enamored with baseball, he once said, "A hot dog at the game beats roast beef at the Ritz."

For many fans of baseball, visiting a stadium is about more than just catching a game. It's considered America's national pastime, and the stands offer the chance to catch-up with old friends and make new connections and memories.

But in 2020, with the COVID-19 pandemic surging and spreading, Major League Baseball (MLB) teams belatedly kicked off their seasons in parks and stadiums with silent stands and empty seats.

"It's surreal to be in Busch Stadium and have a game with no guests," says Phil Melcher, CPP. Prior to the 2020 season, Melcher, security director for the St. Louis Cardinals, estimates that the Missouri ballpark would host roughly 40,000 guests on game nights.

Although MLB was able to provide teams with crowd noise recordings from games in previous seasons and parts of the stands were filled with cardboard cutouts of players, fans, and even dogs and horses, Melcher says it just wasn't the same.

While there was both hope and levity on the field as teams and fans explored new, socially distanced ways to root for teams, Melcher and other stadium security leaders kept their game faces on and began planning to adapt the ballparks and procedures so that fans and employees could safely return.

ST. LOUIS: THE GATEWAY CITY

Busch Stadium is part of a busy downtown neighborhood that usually sees heavy foot traffic regardless of game time.

Across from the stadium is Ballpark Village, with restaurants and bars; the Robert A. Young Federal Building sits two blocks away; within a five-block radius, there's the Gateway Arch and the Historical Courthouse; and about eight blocks from the stadium lies the Enterprise Center, home to the city's National Hockey League (NHL) team, the Blues, and Union Station, with its own attractions, including a Ferris wheel and an aquarium.

"The way I have to look at security, it can't end where my sidewalks end," Melcher says. "It has to extend beyond that because you're looking at the lifeblood of downtown."

He adds that because the neighboring venues are dependent upon the safety of the area, the Cardinals see benefits in being a good neighbor, making connections and forming relationships with nearby businesses. For example, when Melcher conducts a risk assessment for the stadium, he invites these neighbors, "so we have kind of a shared security posture, so we're all benefitting, we're all on the same sheet of music in what we're doing. I think that's really important."

This became even more important in the lead-up to the 2020 season, with Opening Day originally scheduled for 26 March.

But the MLB postponed the season by three months while it worked on protocols for games and players aimed at mitigating exposure to COVID-19, as well as trying to secure a labor agreement with the MLB Players Association. The league cut the number of games from the usual 162 down to 60.

In that interval before the season, Busch Stadium's gates were closed, and approximately 90 percent of staff were ordered to work from home.

But security guards remained at their posts, partly to discourage trespassers because of rising frustrations in the city.

St. Louis was immune to neither the pandemic nor incidents of civil unrest that marked the summer of 2020 in the United States and other countries. The stadium and other businesses became part of the backdrop to rallies for Black Lives Matter demonstrations and protests against law enforcement's use of excessive force.

Some protests turned violent, and day-to-day crime increased, especially as the downtown area was largely devoid of people. There were also incidents of drag racing on city streets and an increase in violent crime with police logging 114 assaults downtown in June 2020 alone, according to *The St. Louis Post-Dispatch*.

Some of the rise in crime could be the result of economic turmoil in the region caused by the pandemic. Melcher says he understands those frustrations and was seeing them firsthand within his second family—the Cardinals organization. No guests at the stadium meant the disappearance of a major revenue stream, which in turn meant that people were laid

THIS IS ALL A
VERY REAL IMPACT
ON SO MANY LEVELS
THAT WE'VE HAD
TO *really rally*
BEHIND EACH
OTHER, *be there*
FOR EACH OTHER.

off from the organization. Melcher, who regularly led in-person awareness and security classes for the team and its staff prior to the pandemic, says that the last year hit them hard. "For us, it's very personal, the losses of people who have since been laid off," he says.

The impacts of the coronavirus on the team have been more than financial, Melcher admits, as the virus killed some stadium employees and former staff. Com-

pounding frustrations further marked the team. In March, Melcher says, he attended a wake for a former member of the stadium's grounds crew who died by suicide.

"This is all a very real impact on so many levels that we've had to really rally behind each other, be there for each other, and let others know, 'Hey, we're here for you if you don't feel right, even if you just need to talk or scream, throw something at the wall. If you need a friend, if you need somebody to be there, I'm here for you,'" Melcher says.

Online and video chat platforms have helped in maintaining communications with staff, not only for support and morale, but also in enhancing security operations while maintaining social distancing. One recent Zoom call included organizers of a local homeless shelter, so the security team could determine how to best interact with an increasing homeless population in downtown St. Louis.

"They may need some other kind of intervention that law enforcement isn't the right call to make," Melcher says.

He adds that he finds these education sessions useful for his team, helping it learn to start a conversation instead of a conflict with at-risk persons.

"Does it come from a position of authority or does it come from a more human perspective where you're trying to relate to them and trying to share some human commonality with them that doesn't denigrate them or make them feel less of a person? It's a safer kind of environment for my security staff as well because it's less confrontational," he says.

From Melcher's view, de-escalation has become more crucial than before. Although fans were not admitted into the stadium for the 2020 season, vehicle traffic was prohibited in surrounding streets for viewing parties with big screens showing the games. Along with protecting guests from more traditional threats—such as drugs or incidents with firearms—security maintained social distancing measures among guests outside.

TORONTO: THE CITY THAT WORKS

For the Blue Jays, home is usually Rogers Centre in downtown Toronto, Ontario,

Canada. But when the Canadian government closed its borders in 2020 to try to lessen the spread of the virus, the team moved to nearby Buffalo, New York, to keep playing against other clubs. And although Buffalo's Sahlen Field sits on the U.S.–Canadian border, the team started out the 2021 season even further away in Florida.

According to Mario Coutinho, vice president of Stadium Operations and Security for the Toronto Blue Jays, the team's security department has made the most of its different settings to test how its pandemic efforts can adjust, depending on regulations and regions.

"Working with the protocols that Major League Baseball has provided to our players, we've developed a pretty comprehensive plan," Coutinho says, adding that he looks forward to applying that plan to



Rogers Centre. "In the meantime, we're adapting that for Florida based on local public health guidance, and also another plan for Buffalo."

While the MLB has established some baseline protocols for clubs, every city and region is different in what they ask citizens and businesses to do. But two areas that Coutinho sees as universally agreed-upon practices among ballparks

PRE-FAB

SECURITY BOOTHS

- ARCHITECTURAL OR INDUSTRIAL
- BULLET RESISTANT OR STANDARD
- THOUSANDS OF DESIGN OPTIONS
- OPTIONAL RESTROOMS AND PLATFORMS

PAR-KUT

INTERNATIONAL

(586) 468-2947

PARKUT.COM

For product info #13 securitymgmt.hotims.com

are cleaning protocols and health checks.

"All our staff—whether you're an usher or a security guard or concession worker—will become health capacitors," Coutinho says. "We'll have to do our part to ensure that everyone sees us going the extra mile to ensure their safety."

Coutinho adds that the pandemic seems to have accelerated the pace of technolog-

THE WAY I HAVE TO LOOK AT SECURITY, *it can't* *end* WHERE MY SIDEWALKS END.

ical developments and adaptation of existing technologies for security protocols. For example, shifting its fans to digital instead of paper tickets offers the team insight into trends that can help it improve the facility.

Coutinho notes that when they return to Rogers Centre, this data analysis will be highly useful—such as for knowing when and where to adjust staff numbers so bottlenecks do not build up at more popular entrances. The stadium's location in the downtown region lacks significant parking spaces for guests, who instead largely use the city's public transportation system. However, on previous game days, this also meant that large numbers of guests arrived in waves and clustered

at entrances, waiting to scan their tickets, walk through a metal detector, and have their bags and persons searched.

Like Busch Stadium, the Blue Jays also maintain partnerships with other groups in Toronto, including law enforcement, emergency responders, CN Tower, Social Bank Arena, Ripley's Aquarium, and the city's transportation departments. This network, which shares information on events and security matters, has allowed for the development of "a unified approach to managing our events," Coutinho says.

The partnership with law enforcement and other city departments means that Coutinho can coordinate on any surveillance of potential threat actors. The stadium's camera system along the perimeter can also assist with monitoring for potential threats and crowd management.

"By testing some of these measures in Florida, it's allowing us to see what works, what doesn't work, where we're focusing our staff and communications strategy, physical markers, messaging," Coutinho says.

PHILADELPHIA: THE CITY OF BROTHERLY LOVE

Before COVID-19 and 2020 had stadium security shifting its focus to pandemic protocols and hygienic thresholds, it was learning from other types of incidents and attacks.

September 11 was the "start of a lot of my colleagues' careers in the sports security role," says Sal DeAngelis, security director for the Philadelphia Phillies. "A lot of us worked in ballpark operations, me included, and when 9/11 happened a lot of us got thrown into a security role, even without a security or law enforcement background. We learned quickly, but we've been honing our craft for the last 20 years."

Subsequent attacks—including the bombing of the Boston Marathon in 2013, a suicide bombing at a concert at Manchester Arena in England in 2017, and the mass shooting at a 2017 music festival in Las Vegas, Nevada—further shifted security postures at sporting and music events.

Along with reacting to new threat tactics, DeAngelis and the rest of the security team

at Citizens Bank Park, where the Phillies play, work on being proactive by researching trends and implementing technologies. Like the other ballparks, they also maintain partnerships and communications with their neighbors, many of whom share similar security challenges.

Citizens Bank Park is part of the Philadelphia Sports Complex, which also includes the Wells Fargo Center, where the city's NHL and National Basketball Association (NBA) teams—the Flyers and 76ers, respectively—play; Lincoln Financial Field, home football stadium for the Eagles; and Xfinity Live!, an entertainment, dining, and shopping center. The security leaders from these sites constantly share information, from suspicious people or vehicles to drug detection to social media monitoring. DeAngelis says that their communication is sometimes informal, but nevertheless effective, crediting the respective organizations for buying into security.

Unlike Busch Stadium and Rogers Centre, Citizens Bank Park is more removed from the city's walkable neighborhoods with shops, restaurants, and bars. But like the other ballpark security leaders, DeAngelis says he understands the importance of relationships with groups based outside of the Sports Complex.

"We're in constant communication with the Philadelphia Police Department," DeAngelis says. His department also regularly connects with the Delaware Valley Intelligence Center, a regional fusion law enforcement monitoring program that gathers, analyzes, and shares threat intelligence.

Beyond regional partnerships, the ballpark's security team is also familiar with U.S. federal agencies—including the FBI, U.S. Department of Homeland Security (DHS), the U.S. Department of State, and the U.S. Secret Service—because, prior to the pandemic, the site was a venue for concerts, outdoor NHL and American Hockey League games, and political events for presidential campaigns.

"I believe they were successful events because of our relationships with our law enforcement partners," DeAngelis says of the non-baseball events. "Nobody is



meeting anybody for the first time when there's an event at Citizens Bank."

THE BEST DEFENSE

Those relationships for Citizens Bank Park and other stadiums are reinforced by security methods and technologies that mimic those seen in critical infrastructure facilities, especially since the stadium secured a SAFETY Act designation from the DHS in 2019.

Through the Support Anti-Terrorism by Fostering Effective Technologies (SAFE-TY) Act, DHS coordinated with the MLB, NFL, and NBA on upgrading stadiums' and arenas' security posture against acts of terrorism.

Bruce Davidson, former director of the Office of SAFETY Act Implementation, said in a statement that achieving SAFETY Act designation or the even more demanding full certification is no small task. Through an evaluation process that includes a site visit during an event, sites must prove the establishment and adherence to best practices for security operations. These include procedures for life safety, evacuations, patron screening, security equipment, delivery/loading dock screening, command and control, security personnel, access control, and training.

Melcher, who began pursuing the designation for Busch Stadium after taking his current position, says he knows that achieving full certification requires the support and a shift in focus for the entire organization. The stadium achieved full certification in September 2019.

"It's an acknowledgement of the work of the organization as a whole," says Melcher, who is now in his fifth season with the team. "It's definitely a holistic kind of approach to security that everybody has to buy into and everybody has to be a part of for it to work."

BATTER UP

As the MLB continues its 2021 season, some things are swinging back into a more normal flow. Both Busch Stadium and Citizens Bank Park have allowed for at least some fans to come back in-person—social distancing and face masks aren't going away anytime soon for the

league—which means that the sites are fully staffed again.

DeAngelis says that for the Phillies there is currently a shift in how staff screen guests and inspect bags, with new limits on what is approved. For the most part, the ballpark is no longer permitting bags or backpacks since searching them could put their staff at risk and make screening a longer process. However, smaller bags, including purses, medical bags, and diaper bags no larger than 16"x16"x8" are permitted. Also, guests are the ones to go through their bags, with security keeping their eyes alert but hands off.

"That's something to help us streamline the screening process," says Coutinho. Back at Rogers Centre, the stadium already instituted a no-bag policy for non-sporting events while the team remains away. It also eliminates the need for staff at gates to come into direct contact with guests.

**WE'LL HAVE TO DO
our part TO
ENSURE THAT
EVERYONE SEES US
GOING THE *extra*
mile TO ENSURE
THEIR SAFETY.**

Other protective measures are working to mitigate crowding at gates—guest capacity is reduced, in accordance with local, state, and league guidelines. This allows facilities to spread out active entrances, avoiding clusters and maintaining social distancing.

Even though vaccination campaigns continue to spread throughout the United States, security leaders are aware that another epidemic or pandemic is a likely reality. So, while the nation's pastime will continue to play out for devoted fans, other traditions linked to the games are unlikely to return—especially traditions that bring fans into close or direct contact with players.

In 1910, U.S. President William Howard Taft threw a ceremonial first pitch at the opening day game for the Washington, D.C., Senators, creating a tradition of presidential first pitches. Since then, nearly every U.S. president has had at least one first pitch on opening day, an All-Star game, or during the World Series. Performers would stand on the field to sing the National Anthem. As players exited the stadium or the field, fans would cluster in the hope of getting an autograph. If a fan caught a ball in the stands, he or she could keep it or throw it back to a player on the field. With new restrictions and security shifts set off by the pandemic, these are all things that might only be seen again if you're watching *Bull Durham*.

In St. Louis, security is spending less time dealing with guests and more time ensuring protocols are followed. Before the coronavirus, people had greater access to the team and the clubhouse—the room or rooms where players can shower and change prior to and after a game. Outside sources' access to the clubhouse is now kept to a minimum to limit the spread of COVID-19.

"Even the media, after a game, would go into the clubhouse and do interviews in the locker area," Melcher recalls. "That ended. That's not going to happen, and I don't know if that will ever come back."

"That's the sad part of this because these teams are such a part of the community regardless of the city," Melcher says. "Sport is definitely kind of a safe place and a place for uplifting society, and people have so much invested in it." ■

Sara Mosqueda is assistant editor at *Security Management*. Connect with her at sara.mosqueda@asisonline.org. Follow her on Twitter: @ximenawrites.

SECURITY TECHNOLOGY



RISE OF THE SURVEILLANCE STATE // By Megan Gates

People in China are among the most surveilled in the world, taking 16 of the top 20 spots on the most surveilled cities list, based on the number of cameras per 1,000 people in an annual assessment from Comparitech published in May 2021.

The analysis found that globally there are already more than 770 million cameras in use, and 54 percent of those cameras are in China. Taiyuan, for instance, has approximately 117 cameras per 1,000 people.

China laid the groundwork for this surveillance network decades ago with community grid management and the Golden Shield Project, which helped local officials and law en-



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

forcement begin their digital transformation of existing surveillance practices.

Now, China has a vast surveillance infrastructure made up from video systems, Internet monitoring, location tracking, and more. And nowhere is the power of this system more on display than in Xinjiang where approximately 13 million Turkic Muslims are monitored through mobile apps, biometric collection, artificial intelligence, big data, and more.

“The mass surveillance programs in Xinjiang are China’s most visible and intrusive, but they are just one end of a spectrum,” wrote Maya Wang, senior China researcher for Human Rights Watch, in an April 2021 piece for *Foreign Affairs*.

“Chinese authorities use technology to control the population all over the country in subtler but still powerful ways,” she wrote. “The central bank is adopting digital currency, which will allow Beijing to surveil—and control—people’s financial transactions. China is building so-called safe cities, which integrate data from intrusive surveillance systems to predict and prevent everything from fires to natural disasters and political dissent.” ■

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



Three Cybersecurity Risk Issues to Consider with Surveillance Systems

RISK ASSESSMENT

By *Elisa Costante*

Connected physical security equipment, like networked surveillance cameras and smart access control systems, offer many advantages for facility and safety managers responsible for securing the premises of retail, industrial, government, and other organizations. Integrated IP-video recording systems with cloud-based recording and administration features are popular among users with little time to purchase and integrate different camera, cabling, and video storage hardware.

Research on this physical security slice of the Internet of Things (IoT) device market and real-world events, however, shows adoption of these systems introduces complex cyber risk issues.



A Global Disconnect: Regulation of Commercial Privacy Practices and Government Surveillance

NATIONAL SECURITY

By *Caitlin Fennessy*

When it comes to international data transfers, the EU's General Data Protection Regulation (GDPR) demands that foreign data protections in the national security sphere be assessed alongside commercial ones. This dichotomy has placed the two issues—commercial data processing and government surveillance—on a collision course. In July 2020, when the Court of Justice of the EU (CJEU) handed down its “Schrems II” decision, the wreckage of yet another crash was strewn globally.

Policymakers and companies around the world are now working to pick up the pieces.



How Drones are Enhancing the Security Toolbox

UNMANNED AERIAL SYSTEMS

By *James A. Acevedo, CPP*

Security, investigative, and executive protection professionals around the world appreciate the evolution and advancement in technology that have added to their everyday carry. But with new operational requirements and threats, professionals need to be creative with the items they add to their daily use.

For instance, the use cases for unmanned systems are only limited to the imagination and the legal operating theater. Despite the myriad of rules and regulations—and the lack of them in some instances—security organizations are beginning to use unmanned aerial systems for surveillance.

SMILE: YOU'RE PROBABLY ON CAMERA

Where in the world is the city with the most surveillance cameras? It depends on how you want to measure, according to analysis by Comparitech, which looked at the number of cameras per square mile versus the number of cameras per 1,000 people when putting together its annual list of most surveilled cities. It found that 16 of the top 20 most surveilled cities—based on cameras per 1,000 people—were in China. Delhi, London, and Chennai lead the categories for cities with the most cameras per square mile. In either case, Comparitech said: “We found little correlation between the number of CCTV cameras and crime or safety.”



Taiyuan, China, had the most cameras per person with 465,255 cameras for 3.96 million people; 117.02 cameras per 1,000 people.



Delhi, India, had the most cameras per square mile with 551,500 cameras for 302 square miles; 1,826.58 cameras per square mile.



Tokyo, Japan, is populated by 37.33 million people but has just 39,504 cameras; 1.06 cameras per 1,000 people and 7.54 cameras per square mile.

Source: *The world's most-surveilled cities*, Comparitech, May 2021

Up Your Game at GSX



The game has changed. So has Global Security Exchange (GSX). Taking place 27-29 September, GSX is designed to meet your needs—offering global security practitioners a new hybrid experience from the largest association for security management professionals. GSX will be held both online and in-person at the Orange County Convention Center (OCCC) in Orlando, Florida, USA.

GSX is a pro's playbook to security's most important topics. With sessions focused on preparing for the unexpected, withstanding an attack, building and motivating teams, attracting and retaining skilled employees, what's next for security, navigating the growing security industry, and more, the GSX education lineup has something for professionals at any level in their career.

GSX in-person offers All-Access attendees six themed learning theaters and 80+ live sessions, including inspiring education sessions, expert-led tracks, exhibitor presentations, timely general sessions, and digital content available before, during, and after the on-site event. All-Access attendees, whether in-person or digital, can earn up to 21 CPEs toward their recertification.

Digital attendees can enjoy live broadcasts from two of the theaters, with the top attended sessions from the remaining theaters becoming available after the live event. Digital attendees will be able to chat live with in-person attendees and even ask the speakers questions.

ASIS International's top priority is the health and safety of GSX stakeholders. The OCCC is one of the largest venues in the United States to receive the Global Biorisk Advisory Council® (GBAC) STAR™ accreditation, recognized as the third-party gold standard in cleanliness and disease prevention. ASIS is also partnering with Safe Expo, the preeminent service provider for pre-event health planning support, onsite implementation, and post-event health monitoring.

Learn more about GSX health and safety protocols and register for an All-Access pass at [GSX.org](https://www.asisonline.org/GSX.org).

ASIS Global Governance: 2022 Update

ASIS International is poised to take the next major step in its transition to a global governance structure that allows the organization to provide better service to its members at the local, regional, and global levels. Beginning in 2022, ASIS will stand up regional boards of directors in both the European and North American regions, with plans for additional regional advisory committees to be seated in future years.

The active chairs of both the European Regional Board (which will seat eight directors) and the North American Regional Board (which will seat 12 directors) will serve on the ASIS Global Board of Directors. These regional boards' representation on the Global Board will begin in their first year of operation, in 2022.

In keeping with recommendations by ASIS's European and North American governance workstreams, half of the inaugural members of each regional board will be appointed by the Global Board of Directors.

A European Regional Board Nominating Committee, consisting of ASIS's Global Board of Directors Nominating Committee and three Global Board-appointed European members, will select the remaining participants for the European Regional Board from a pool of European members who have submitted candidate interest forms for consideration to serve. Likewise, a North American Regional Board Nominating Committee consisting of the Global Board Nominating Committee and three Global Board-appointed North American members will similarly select North American members to serve on the North American Regional Board.

ASIS will begin accepting candidate interest forms from individuals in Europe and North America in late July. Forms will be due in early September. Visit the Global Governance page on the ASIS website for the latest updates.

This new governance structure, which began with the seating of the first Global Board of Directors in 2020, marks a new era for ASIS International—reflecting the diversity of geography, thought, specialty, age, market vertical, and experience of our global membership.

For the latest information on ASIS Governance, visit [asisonline.org/GlobalGovernance](https://www.asisonline.org/GlobalGovernance).

Updated POA Now Available

To keep pace with the evolving security industry, in May ASIS released an update to the *Protection of Assets* (POA) reference set. Refreshed to reflect our changing times and keep security professionals on the leading edge of best practices in the field, this collection is designed to assist security management directors and professionals responsible for corporate asset protection.



This updated reference set—which was first published in 1974—is considered the security industry’s premier resource. Written, edited, and revised by hundreds of veteran subject matter experts across the security continuum, the POA constitutes recommended reading for all four of ASIS’s certifications.

Available individually or as a bundle, the POA includes vital learning on the following aspects of asset protection:

- **Business Principles**, including the fundamentals of security business operations, management, and leadership.
- **Crisis Management**, including emergency management, business continuity, and crisis communications.
- **Personnel**, including security officer operations, employee drug testing, executive protection, and spotting problematic behavior.
- **Physical Security**, including design principles and practices, tools and techniques to satisfy protection objectives, and practical project management guidance.
- **Investigations**, including interviews and interrogations, undercover investigations, due diligence, preemployment background screening, evidence collection, and expert testimony.
- **Security Management**, including theft and fraud prevention, security standards, loss reporting, methods, and enterprise security risk management (ESRM).

ASIS members can enjoy a discount of \$200 off the list price and free global shipping on the softcover bundle. Learn more about the *Protection of Assets* at asisonline.org/PoA.

Young Professionals Corner

Meet ASIS Young Professionals Community Steering Committee Secretary Dustin Wilhoit and participant Codee Ludbey, CPP.

Dustin Wilhoit

Young professionals can stand out in this industry by speaking less, listening more, and taking advice from everyone. Take the good advice and build upon it. Take the bad advice and change it to work. Always be willing to step up to any task thrown your way, and think and work outside of the box. Be innovative, not typical.



Codee Ludbey, CPP

Security is a truly multidisciplinary field of expertise that requires quick but deep thinking about some of the most pressing social challenges we face as a global society. I enjoy working in the security field because it requires me to think laterally about how to achieve security outcomes while balancing public amenity, community expectations, and a functional asset. Locking everything up isn’t always practical!



Member Book Review

Crisis Negotiations: Managing Critical Incidents and Hostage Situations in Law Enforcement and Corrections. By Michael J. McMains, Wayman C. Mullins, & Andrew T. Young, Routledge; Routledge.com; 602 pages; \$64.95.

This book represents a comprehensive treatise of the discipline of crisis negotiations. It is well-suited to serve as a textbook in a college or university course.

Each chapter includes thought-provoking discussion questions and access to support

ASIS Global Board OF DIRECTORS

PRESIDENT

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

PRESIDENT-ELECT

Malcolm C. Smith, CPP
Qatar Museums
Doha, Qatar

SECRETARY/TREASURER

Timothy M. McCreight, CPP
Canadian Pacific Railway
Calgary, Alberta, Canada

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

Joe M. Olivarez, Jr.
Jacobs
Houston, Texas, USA

Axel Petri
Deutsche Telekom AG
Bonn, Germany

Malcolm B. Reid, CPP
Brison
Richmond, Virginia, USA

Chiko Scozzafava
Ewa Beach, Hawaii, USA

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

EX-OFFICIO VOTING

Scott A. Lowther, CPP, PCI
PetroChina
Rocky View County, Alberta, Canada

Cy A. Oatridge, CPP
OSG
Tacoma, Washington, USA

EX-OFFICIO NON-VOTING

Bernard D. Greenawalt, CPP
Retired
Tinley Park, Illinois, USA

Kristiina Mellin, CPP, PCI, PSP
Accenture
Tyresö, Sweden

materials including slide presentations and test banks.

More importantly, it is essential reading for practitioners in crisis negotiations. The book includes a thorough history and development of the discipline, negotiation techniques, risk assessment, and crisis management guidelines. It also addresses negotiation techniques for various special populations, such as emotionally disturbed or mentally ill peo-

ple, juveniles, elderly, combat veterans, and law enforcement.

All three authors are not only university professors, but also have extensive field experience in crisis negotiations. It is clear through their writing that they not only have the academic knowledge, but also practical field experience in the discipline.

Other suggested uses of the textbook by practitioners would be as a reference guide

in the field during negotiations, initial training of newly assigned negotiators, and as a source for ongoing training for all assigned negotiators.

The authors have interjected numerous case studies and negotiator profiles throughout the text. These elements provide additional valuable learning opportunities for the student and practitioner. They bring the principles of negotiation to life for the reader.

The content of *Crisis Negotiations* is well-organized and easy to read. The book clearly illustrates that the discipline has evolved since its inception about 50 years ago. It is a highly recommended resource for any student or practitioner of crisis negotiations.

Reviewer: Dennis Eberly, MS, LPI (Licensed Private Investigator), is the owner of On Target Investigation & Consulting, LLC. He retired as a police lieutenant from the East Hempfield Township Police Department in Lancaster County, Pennsylvania, after 33 years of service. Eberly also served as a Negotiation Unit Supervisor for the Lancaster County Special Emergency Response Team (SERT). He has held criminal justice faculty positions at several institutions over the past three decades. ■



#MYASIS IMAGE OF THE MONTH

Pablo Colombres, CPP

Supporting ASIS International Chapter Portugal kick off! Congratulations to the security colleagues from Portugal who have chosen to become part of the world's largest membership organization for security management professionals.



ASIS CERTIFICATION PROFILE // KEVIN SMITH, CPP, PCI, PSP

Kevin Smith transitioned into a security management career after seven years in law enforcement. Now an enterprise security specialist for a utilities provider in Colorado, he finds himself drawn to the security function's ability to create positive outcomes for an organization—from top to bottom.

With approximately 20 security officers reporting directly to him, Smith and his team monitor all events that may pose a threat to the organization's operations. With such an important mandate, Smith finds that adhering to industry-proven best practices is an effective way to ensure success.

"My mentor introduced me to ASIS," he shares. "My member-



ship has connected me with security professionals around the world who share the common goal of protecting individuals, wherever they may work. Those connections have helped shape the services, programs, and procedures that I have brought back to my organization."

He earned ASIS International's Certified Protection Professional (CPP®) certification in 2010, following the lead of his triple-certified mentor. "Part of the value of becoming certified is the invaluable knowledge you gain from your study and preparations," he says. "My organization supported me in pursuing my certifications because they understand the value this knowledge brings to the organization."

Now, Smith holds the ASIS International Triple Crown, having earned the CPP, the Professional Certified Investigator (PCI®), and the Physical Security Professional (PSP®) certifications. He shares his knowledge as an adjunct professor for the Metropolitan State University of Denver, an instruc-

tor for the ASIS Asset Protection Course, and as a contributor to the Investigations section of the newly revised *Protection of Assets (POA)* reference set.

An especially memorable moment for Smith came when he and his team rolled out a new workplace violence protection program for the organization.

"Security offers you the opportunity to shape the minds, culture, and, ultimately, behavior of others with the goal of creating and maintaining a safe environment," he reflects. "This field allows you to explore creative and proactive ways to help mitigate threats in our ever-changing world."

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

VIDEO MANAGEMENT

Interface Security Systems announced that restaurant chain El Pollo Loco is relying on its managed video verified alarms and intrusion alarm monitoring. The system allows restaurant security to detect intrusions and minimize false alarms. The service included replacing outdated alarm systems with new ones, plus Interface's 360 Alarm Maintenance Service, which ensures all maintenance issues involving duress buttons, connectivity, or the alarm panels are addressed. Annual technical inspections ensure the alarm systems always remain operational. A pilot project revealed that with every alarm event, Interface's remote monitoring team would verify whether the alarm required a call to local law enforcement. Only 5 percent of such events required police involvement, while the rest were false alarms, saving El Pollo Loco thousands of dollars by cutting down false alarm penalties and associated costs.

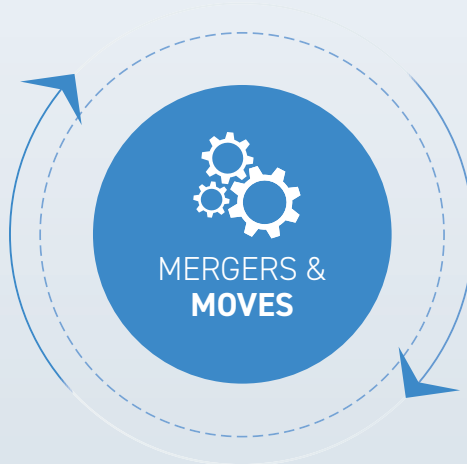


Appspan Security ➦ Xpandion

Appspan's acquisition of the company will provide an integrated approach to automating authorization lifecycles and controlling access to sensitive business data.

Hexagon AB ➦ CADLM SAS

Hexagon will use CADLM's products and processes to improve product design innovation, manufacturing productivity, and product quality.



IMG Companies, LLC ➦ INTA Technologies Corporation

The acquisition advances IMG's growth plan and customer diversification in target sectors, as well as enhancing manufacturing.

HelpSystems ➦ Beyond Security

The acquisition allows HelpSystems to expand its infrastructure protection portfolio, which already includes Digital Defense, Core Security, and Cobalt Strike.



Award

SecurityHQ received a 2021 IBM Beacon Award in the Outstanding Security Solution category for its Incident Management & Analytics Platform, in recognition of its use of IBM technology to innovate a solution for clients.



Contract

March Networks will provide mobile surveillance for the California Transportation Agency's fleet of more than 400 buses and up to seven years of cloud-based monitoring services.



Announcements

Gilbane Building Company selected AMAG Technology's Symmetry Security Management System to deploy at the new Hines 100 Mill commercial high rise in Tempe, Arizona.

Partnerships



Smart Cars

Vehicle cybersecurity provider AUTOCRYPT partnered with SHIELD Automotive Cybersecurity Centre of Excellence to prioritize research and development in securing connected and autonomous vehicles.

Digital Forensics

MSAB and Detego announced a strategic partnership that will offer users a site to acquire data for both mobile and computer analysis, plus a complete end-to-end suite of modular digital forensics tools.

Cybersecurity

XM Cyber entered into an agreement with Spire Solutions, allowing for expansion into Israeli and Middle Eastern markets.

PRODUCT SHOWCASE



SURVEILLANCE CAMERAS

The **Hanwha Techwin** PNV – A9081R camera is an artificial intelligence, IR outdoor vandal dome camera that captures images up to 4K resolution, while also including powerful, in-camera deep learning algorithms. Utilizing object recognition versus motion detection all but eliminates false alarms while also providing valuable business and operations insight. These AI cameras also offer performance in both analytics and deep learning applications. The included license-free analytics detect and classify a range of objects including people, vehicles, license plates, and faces. This technology can also provide a reliable edge-based intelligence. Visit www.hanwhasecurity.com/pnv-a9081r.html to learn more. **Circle 101**

WIRELESS ETHERNET

ComNet Communications Networks is introducing its new Generation 4 Net-Wave wireless products, which offer greater performance in applications where throughput is a challenge. The NW1 Gen 4 can exceed 500Mbps, accommodates 10/100/1000Mbps Ethernet, and it also now has IEEE802.3at PoE Compliant PD on port 1 and an IEEE802.3af power source (PSE) available on port 2. The new hardware features a high-performance chipset with a quadcore CPU that is designed to meet the high throughput demands that surveillance applications require. Visit www.comnet.net/comnet-products/ethernet/wireless/5ghz-wireless-ethernet/nw1-gen4 to learn more. **Circle 102**



StarLink Fire



EMERGENCY RADIOS

With **StarLink Fire** Cellular Communicators, clients can ensure they will have a fast emergency and fire alarm response when weather events or telephone companies cut off leased landlines, which are already starting to disappear in parts of the United States. Clients can upgrade a fire alarm that is reliant upon old communication technologies, making it code compliant with these universal cellular or cell/IP solutions for Commercial Fire. StarLink Fire Radios can communicate either on AT&T or Verizon networks and offer users a chance to save thousands of dollars compared to landlines. Visit www.starlinklte.com to learn more.

Stand 12031, Circle 103

OUTDOOR LOCKING BAR

Detex is the only manufacturer of the outdoor latch retraction device, a solution that can be used in a variety of environments, including corporate facilities, gated complexes, outdoor entertainment, dorms, stadiums, and more. Unlike electromagnetic locks, this outdoor locking solution can remain locked when there is a power loss. Those protected by the locking device can always push upon the need to exit, while no unauthorized outsiders can pull on it in order to get into the protected room. Visit www.detex.com/ISCW to learn more. **Stand 12092, Circle 104**



SCREENING LANES

Evolv Technology offers a patented solution that enables venues all over the world to deploy touchless screening technologies for weapons detection, identity verification, and health-related threats. Built on top of the Evolv Cortex AI platform, Evolv Express improves visitor flow 10 times faster than metal detectors and, using sensors and artificial intelligence, instantly differentiates personal items from concealed threats like weapons and explosives. Visit [evolvtechnology.com/evolv-express/](https://www.evolvtechnology.com/evolv-express/) to learn more. **Stand 13059, Circle 105**



VEHICLE SURVEILLANCE

ISS's SecurOS Under Vehicle Surveillance System (UVSS) combines software and hardware for under-vehicle surveillance. The solution is developed with various ISS patents and designed to integrate with ISS's SecurOS v10 platform. The SecurOS UVSS also creates a database of high-resolution images of vehicle undercarriages and recognizes vehicle license plates, making it applicable for numerous venues where underground parking or structured parking facilities are used. The system can monitor vehicles with high precision and can be deployed virtually out of the box when interfaced with the ISS SecurOS VMS. Visit www.issivs.com to learn more. **Stand 8077, Circle 106**



ENTERPRISE SECURITY

Maxxess Systems offers complete enterprise security solutions with increased situational awareness and coordinated responses for all markets. These solutions deliver features such as COVID control, integrated mass communication, situation assessments, monitoring at-risk users, multiform panic buttons, and more within a unified security management platform. The open architecture solutions integrate with more than 70 third-party manufacturers in video surveillance, fire systems, intrusion detection, and other industries to meet project requirements. These solutions are customizable with no code changes, and implementation is fast and easy. Visit www.maxxess-systems.com to learn more. **Stand 8077, Circle 107**



IR SURVEILLANCE

The **Pelco Spectra Enhanced 7 Series IR Look Up PTZ camera** offers users wide area coverage, high-speed tracking, and long-range details in unilluminated areas. Able to look up above the horizon and utilize automated infrared illumination, this next generation of cameras allows security operators to monitor large areas, as well as the ability to see in the dark so no incident is missed. Featuring 2MP and 30x optical zoom, the camera series provides top tier image quality, performance, and intelligent embedded features for critical infrastructures such as cities, bridges, roadways, ports, stadiums, and transportation systems. Visit www.pelco.com/products/cameras/ptz-cameras/spectra-enhanced-7-ir-lookup/ to learn more. **Circle 108**



EVENT MANAGEMENT

Everbridge helps manage critical events for more than 5,600 customers across the world, reaching more than 700 million people in over 200 countries, reservations, and territories. Visit www.everbridge.com/platform/critical-event-management/ to learn more. **Stand 5036, Circle 109**



RECORDERS

Speco is introducing the new Recurring Monthly Revenue (RMR) feature for its NRE series recorders. The RMR feature allows Speco customers to pay for the features they need on a monthly basis. This provides the user with an additional monthly revenue stream from a single recorder at no additional cost to the client. Setting up is easy enough, as clients can simply download and register through the Speco Blue Manager App, then quickly select which features the customers can access. Visit www.specotech.com to learn more. **Stand 23017, Circle 110**

specotech.com to learn more. **Stand 23017, Circle 110**

ASSET MONITORING

Users can level-up their GSOC with artificial intelligence-powered crisis alerts and asset monitoring by **samdesk**, which can provide notifications any time a crisis event occurs near a client's assets, even while on the go. Users can get the full picture as it is happening, with access to live updates on local traffic, weather, air quality, and more. Alerts can also be customized by event type, region, level of severity, and more. With alerts on disruption events, users can react faster and respond with confidence. Samdesk offers more signal and less noise so users can protect their people, assets, and brands. Visit www.samdesk.io to learn more. **Circle 111**



DOOR DESIGN

Door hardware and physical security have had a traditionally complicated and challenging relationship, but with **ZBeta**, clients can automate design standards and tame the door hardware beast. Learn how ZBeta's unique design technology can automate security standards and use requirements data to improve the relationship moving forward. ZBeta offers a technology solution that organizes requirements data, helps automate the application of security policies and standards to design projects, and results in dramatically better project results. Visit www.zbeta.com to learn more. **Circle 112**

SURVEILLANCE CAMERAS

Panasonic I-PRO Sensing Solutions announces its new S-series line of cameras. The new S-series offers clients high-quality images thanks to technical advancements. Bundled with built-in artificial intelligence, the high-precision analysis helps simplify surveillance operations, which in turn can improve crime prevention. Three indoor models are scheduled for release in June 2021, and two exterior camera models will be released in September 2021. Every S-series camera comes with a five-year warranty and Video Insight camera license. Visit i-pro.com to learn more. **Circle 113**



SOC MANAGEMENT

Vector Flow's Physical Security Operation Center (SOC) Automation Suite uses deep artificial intelligence-based automation of SOC operations, autonomous alarm reduction, and real-time insights across multiple functions to enhance security operations. Vector Flow's customers see a return on investment from three enterprise software modules: SOC Alarm Reduction Manager, SOC KPI Manager, and SOC Predictive Maintenance Manager. SOC Automation Suite has proven to reduce cost and risk by eliminating up to 80 percent of false or nuisance alarms, automating repetitive tasks, and proactively managing security infrastructure while helping deliver more SOC services, such as COVID-related reopenings. Visit www.vectorflow.com to learn more. **Circle 114**





FACILITY MANAGEMENT

Continental Access has evolved into a developer of smart security and facility management solutions. It offers a wide variety of solutions, including enterprise, mobile, cellular, cloud, wireless locks, and embedded solutions. Continental's flagship CA4K Enterprise Security and Access Control Management Platform is a scalable access control and security platform designed to provide a single flexible, interoperable, integrated security solution. Its CA4K Access Manager App acts as a Virtual Enterprise Workstation on any smart device. New additions to the Continental solutions line-up include E-Access Embedded Solutions and Bluetooth Readers and Air Access cellular-based access control. Visit www.cicaccess.com to learn more. **Stand 12031, Circle 115**

GUARD BOOTHS

Par-Kut International offers clients the design and production of built-to-order, factory assembled security guard shelters. Its welded steel security booths, with standard climate control, can be found at access control points around the world. Model designs range from basic to high-end architectural and all points in between. Sizes range from small, single-officer booths to multi-room and multi-module buildings. Built-in restrooms



are available in booths for facilities that demand constant vigilance over operations. Other features include bullet-resistance, camera and data preps, custom countertops, and platform or trailer mounting. Visit www.guard-booth.net to learn more. **Circle 116**

ACCESS CONTROL

This optical security device from **Designed Security, Inc.**, using proprietary sensing technology to detect direction and tailgating, is suited for areas requiring tighter security. Compatible with all card reader technologies and access control systems, the Entry Sentry helps to ensure that only one individual enters through a secured doorway for each valid authorization, preventing tailgating. Its design does not detract from interior aesthetics and mounts easily on standard door frames and hallway walls. Entry Sentry consists of two self-contained, narrow door/wall mounted units providing both local and remote alarm indications. Visit www.dsigo.com/PSSMo7 to learn more.

Stand 12092, Circle 117



STORAGE OPERATING SYSTEM

Dell Technologies has teamed up with VMS partners to reduce the risks associated with deploying safety and security solutions. Easier to manage and maintain, the PowerScale OneFS OS enables a single volume, shared by all the camera streams.

The solution offers scalability and performance, and it is able to increase capacity in seconds by simply adding another node, meaning no downtime or disruption. PowerScale also offers enterprise-level data protection and can help organizations deploy big data analytics faster and with less cost. Visit www.delltechnologies.com/en-ca/storage/powerscale.htm to learn more. **Circle 118**



Brownguard®

INSURANCE COVERAGE

The **Brownard Group's** Brownguard Insurance Program has served and protected the interests of security professionals for more than 70 years. The Brownard family continues to affirm its commitment to the security industry by supporting the Intrepid Fallen Heroes Fund. Visit www.brownguardins.com/quote-request/ to learn more. **Circle 119**



KEY CONTROL

Morse Watchmans is the original developer of electronic key control. Clients can manage all facility keys with the Morse Watchmans KeyWatcher Touch. Users can also design and customize a system by selecting from several module options that secure keys and key rings, as well as lockers that secure assets such as wallets, cell phones, and laptops. The KeyWatcher Touch is expandable and can be integrated with other access control systems for enhanced security. All products are made entirely in the United States, and Morse Watchmans has distributors around the world. Visit www.morsewatchmans.com/products/keywatcher-touch to learn more. **Stand 12109, Circle 120**

SAFETY LOCKSETS

Marks USA LifeSaver ANSI Grade 1 institutional life safety locksets address managed liability accident prevention, life safety, and security in behavioral health care institutions, X-ray settings, and correctional facilities. LifeSaver offers a number of variations—cylindrical, mortise styles, models, and functions are available, including electrified units, which can work on buzz-in and man-trap settings, plus GermAway antimicrobial finishes. Also,



the 5-Point Ligature-Resistant Slide Health models, an option for institutional and corrections applications, meet the latest BHMA 156.34 anti-ligature trim standard and are approved by the Joint Commission (JCAHO). Marks' products are backed by the Marks exclusive lifetime mechanical warranty. Visit www.marksusa.com to learn more.

Stand 12031, Circle 121

LOCK CONTROLS

Dortronics' 48900 PLC Interlock Controller offers a solution for implementing door interlock systems with up to nine doors. The fully integrated, single-board solution provides installers with complete control of all operating and configuration options without the need and expense of complex software. The 48900 Series Controller integrates with virtually any access control system utilizing dry contacts. The unit also provides outputs for traffic lights, door violation alarm, and three individual timing sequences for propped door time, emergency override unlock, and request-to-exit unlock time. Visit www.dortronics.com to learn more.

Stand 12140, Circle 123



SURVEILLANCE SYSTEM

At the core of **Hanwha Techwin's** product development is the Wisenet 7 System on a Chip (SoC). Developed in-house and built in Korea, Hanwha Techwin continually enables new features and analytics. With its own device certificate issuing system, Root CA, the Wisenet 7 camera lineup offers the highest levels of cybersecurity possible. Hanwha Techwin's cybersecurity policy embeds unique certificates into all products during each step of the development and manufacturing process, resulting in a cybersecurity policy that satisfies stringent UL CAP standards, plus Hanwha's own requirements for product reliability and design innovation. Visit www2.hanwhasecurity.com/wisenet-7/ to learn more. **Circle 122**

PERIMETER FENCING

Ameristar's Matrix Alpha allows the user to define the level of security needed by choosing a suitable mesh option that details the degree of delay and site visibility. Available in hot-dip galvanized or PermaCoat finish, this fence system is a baseline for perimeter security. The curtain-wall architecture allows for variable post spacing, resulting in reduced installation times. The Exodus Pedestrian Egress Gate system is designed to mitigate multiple trips to the jobsite. This all-in-one gate system has all the required panic exit device hardware preinstalled. Visit www.ameristarfence.com/en/products/fence-systems/matrix-alpha-curtain-wall/ to learn more. **Stand 9073, Circle 124**



TROVE^{PLUS}

POWER DISTRIBUTOR

Altronix's Trove Plus series combines preconfigured power distribution and control supporting the leading access brands, as well as with wire harnesses for controllers and finger duct for wire management. These features allow for an easier and cleaner installation. The series also has a new option that accommodates even more doors in a Trove3 system, utilizing angled brackets to include more power and control in a single enclosure for a client's largest access applications. Altronix products are both NDAA and TAA compliant, manufactured in the United States, and backed by a lifetime warranty. Visit trove.altronix.com to learn more. **Circle 125**

BODY CAMERAS

The **AXIS** Body Worn Solution offers users a way to capture valuable evidence, deter bad behaviors, and positively influence the actions of both the camera wearers and the public. Designed on an open system architecture, which allows for integration with other video management systems (VMS) and evidence management systems (EMS), this solution is highly flexible. Rugged and lightweight, it consists of the AXIS W100 Body Worn Camera, AXIS W800 System Controller, and the 1-bay AXIS W700 or 8-bay AXIS W701



Docking Station. The solution's cameras are easy to use and deliver sharp audio and video recordings. Visit www.axis.com/products/wearables to learn more.

Stand 14051, Circle 126

VISITOR MANAGEMENT

With **AlertEnterprise** Visitor Identity Management, the user can control the full visitor lifecycle, from arrival to departure. On-site registration offers fast processes, including COVID-19-specific attestation; email and Web pre-registration; self-service kiosks; and optional facial recognition technology for a frictionless experience on the customer end. With real-time vetting against watchlists and policy-driven background checks, visitors and contractors are validated before gaining access. Integrated audits and reporting workflows provide automatic compliance enforcement in meeting all standards and regulations. Visit alertenterprise.com/products/enterprise-visitor-identity-management/ to learn more. **Stand 3077, Circle 127**



LOSS PREVENTION SERVICES

Metro One has offered professional security services since 1984. With decades of combined loss prevention and security management experience, Metro One can tailor its service to fully integrate into the client's loss prevention and security program, as well as play a key role in obtaining their objectives, while providing a return on investment. The firm offers recruiting, training, and program development of its loss prevention officers. Visit www.metroonelpsg.com to learn more. **Circle 129**



TURNSTILES

From **Boon Edam**, the Speedlane Compact offers the safety and security of a security turnstile in a smaller footprint. Featuring an ergonomic design, the short V-shaped cabinet optimizes the use of valuable floorspace and the smooth, swing-motion glass barriers can coordinate with any existing building décor and design. The Speedlane Compact also offers standard tailgating, safety, and object detection sensors, which can relieve pressure on security and reception staff as well as offer flexible lane configurations, easy installation, and user intuitive guidance. Visit www.boonedam.com/en-us/products/optical-turnstiles/speedlane-compact to learn more. **Stand 8037, Circle 128**





Conspiracy. Russian national Egor Igorevich Kriuchkov was sentenced to 10 months in prison and a \$14,825 fine in restitution for attempting to recruit a Tesla employee to introduce malware into the company’s computer network.

Kriuchkov pled guilty to one charge of conspiracy to intentionally cause damage to a protected computer on 18 March 2021. He initially pled not guilty in September 2020.

Along with his co-conspirators, Kriuchkov planned to introduce malware to extract data from Tesla’s network. They would then extort the company by threatening to publish the information online unless Tesla paid a ransom.

Kriuchkov approached a Tesla employee based in Nevada, worked to establish a rapport, and eventually offered to pay the employee \$500,000—later agreeing to increase the payment to \$1 million in Bitcoin—in exchange for introducing the malware onto Tesla’s network. The employee reported Kriuchkov’s offer to the company, which notified the FBI.

According to court documents, the attack would have been two-pronged. The first would have appeared to be an external DDoS attack, distracting cybersecurity staff from the second attack that would exfiltrate data from the network. Kriuchkov and his co-conspirators also allegedly targeted other companies through similar methods, notably ransomware.

Since Kriuchkov had already spent nine months in custody, his sentencing in May was nearly tantamount to time served. He will be deported but will be placed under federal supervision for three years if he instead remains in or upon his return to the United States. (*United States v. Egor Igorevich Kriuchkov*, U.S. District Court District of Nevada, No. 3:20-mj-83-WGC, 2021)

Domestic terrorism. A U.S. federal judge sentenced Richard Holzer to 19-and-a-half years in prison for plotting an attack on a synagogue in Pueblo, Colorado.

Holzer pled guilty to a federal hate crime charge and actions that amounted to domestic terrorism, according to the U.S. Department of Justice (DOJ). He planned to use fire and explosives to destroy Temple Emanuel Synagogue on 2 November 2019 and “obstruct persons in the enjoyment of their free exercise of religious beliefs,” according to court documents.

Holzer, a self-identified Neo-Nazi and white supremacist, used social media to promote racist ideologies and violence. An undercover federal agent contacted Holzer through social media in 2019 and determined he was targeting the temple in preparation for a racial holy war. (*United States v. Richard Holzer*, U.S. District Court for the District of Colorado, No. 19-mj-00246-NYW, 2021)

Sexual harassment. A resort business with athletic and leisure facilities in California and Oregon will pay \$500,000 and other relief to settle a sexual harassment and retaliation lawsuit filed by the U.S. Equal Employment Opportunity Commission.

According to the lawsuit, female employees of the Bay Club Company were sexually harassed by customers and managers. The suit also claimed that managers in at least one location retaliated against employees who complained about harassment. (*EEOC v. Bay Club Fairbanks Ranch, LLC, et al.*, U.S. District Court for the Southern District of California, No. 3:18-cv-01853-W-AGS, 2021)

Legislation

United States

Sexual assault. The U.S. House of Representatives reauthorized the Violence Against Women Act (HR 1620), which would protect and provide resources for victims of domestic abuse and sexual violence. The bill awaits a vote from the U.S. Senate.

The law was expired in 2018 when Congress was unable to reach an agreement over certain



COURT CASES

Issue: Domestic terrorism
Case: *United States v. Siesser*
Venue: Western Dist. Ct. of Missouri
Status: Sentenced
Significance: Jason Siesser was sentenced to 12 years in prison for trying to buy a chemical weapon on the Dark Web.

Issue: Cybersecurity
Case: *United States v. Kher*
Venue: Southern Dist. Ct. of California
Status: Sentenced
Significance: Deepanshu Kher was sentenced to 24 months in prison for deleting user accounts from his former employer’s server.

issues, notably language regarding restrictions on firearms and protections for transgender people.

Excessive force. Maryland enacted new accountability measures for law enforcement officers, repealing the U.S. state's Law Enforcement Officers' Bill of Rights.

The Democratic-controlled legislature passed the Maryland Police Accountability Act (MD HB0670) a second time after Republican Governor Larry Hogan vetoed it.

"The original intent of these bills appears to have been overtaken by political agendas that do not serve the public safety interests of the citizens of Maryland," Hogan said in a letter to the leaders of the state House and Senate. The bills "will result in great damage to police recruitment and retention, posing significant risks to public safety throughout our state."

The law, one piece of a four-part reform package, introduces rules on authorized use force, investigations into such incidents, and disciplinary procedures for officers found violating the new rules. Police convicted of using excessive of force can face additional criminal penalties, including up to 10 years in prison.

Other aspects of the law include granting public access to complaints lodged against officers and internal affairs files. There will also be new thresholds for securing permission to raid homes after dark and for "no-knock" warrants, such as signatures from both a police supervisor and the state's attorney.

Regulations

China

Antitrust. China's market watchdog group, the State Administration for Market Regulation (SAMR), issued an 18.2-billion yuan (\$2.8 billion) fine against e-vendor Alibaba for violating competition laws.

SAMR said in a statement that the fine comes after a four-month investigation into the online commerce company and its "abuse of market dominance." The investigation de-



International Regulations

The Netherlands

Data breach. The Dutch Data Protection Authority (DPA) fined Booking.com €475,000 (\$577,439) for belatedly reporting a data breach where hackers accessed the personal data of more than 4,000 customers. The hackers also mined credit card data of 283 victims and were able to collect credit card security codes in 97 instances.

The online travel agency did not report the incident until 22 days after it occurred on 13 January 2019, long past the 22-hour deadline.



The DPA noted that even in instances where credit card information was not compromised, users' leaked personal information could still be used by hackers in phishing attempts. These potential attacks would appear more credible if a scammer had access to information on booking dates and exact locations of previous trips.

Site users were notified of the breach three days before the DPA, and the company attempted to mitigate the damage, including offering compensation.

Although Booking.com is headquartered in The Netherlands, it operates internationally and attracts customers from various countries; the Dutch DPA coordinated with other European privacy regulators in investigating the violations.

termined that Alibaba made its vendors "pick sides"—pushing out its competitors by forcing those selling on its marketplace to choose either Alibaba or rivals' services.

The fine, equivalent to 4 percent of Alibaba's domestic sales revenue in 2019, sets a record for antitrust fines issued in China—three times as high as the previous one against Qualcomm in 2013, according to the *Financial Review*. (Administrative penalty decision, State Administration for Market Regulation, No. 28, 2021)

United States

Aircraft safety. The U.S. Federal Aviation Administration (FAA) levied a \$5.4 million fine against Boeing Company for failing to adhere to the terms of a 2015 agreement intended to renovate the company's culture and attitude towards safety.

In the agreement, Boeing promised to improve and prioritize its internal safety check processes in line with regulatory requirements. Boeing entered the agreement with the FAA, resolving multiple civil penalties against the company. The regulatory pressure focused on the manufacturer was due to compliance issues, although there were no accusations from the agency that Boeing was creating unsafe conditions.

Boeing missed improvement targets outlined in the agreement, and some managers failed to prioritize adherence to federal regulations.

Boeing also agreed to settle two FAA enforcement cases for \$1.2 million. One of the cases alleged that the company failed to properly implement an FAA-approved Organization Designation Authorization (ODA) program while also interfering with members of that program. The second case claimed the company did not adhere to quality-control processes and interfered with safety inspections of aircraft. In both instances the FAA determined that members of the ODA program still fulfilled their responsibilities.

Prior to the fine, and as a condition of the original 2015 agreement, Boeing paid \$12 million in civil penalties. (Settlement Agreement, U.S. Department of Transportation, Federal Aviation Administration, Office of Regional Counsel, 2015) ■

LEGISLATION

Issue: Privacy

Case: In re Facebook

Venue: Northern Dist. Ct. of California

Status: Settled

Significance: Facebook will pay \$650 million for unauthorized collection of biometric information.

Issue: Marijuana

Bill: SB1406

Venue: Virginia

Status: Enacted

Significance: Legalizes possession of up to 1 ounce of marijuana for adults 21 and older. Sales remain illegal.

Issue: Immigration

Bill: Immigration (Amendment) Bill 2020

Venue: Hong Kong

Status: Effective 1 August

Significance: Officials can bar people from entering or leaving Hong Kong, like mainland travel bans used to trap dissidents.

MARKETPLACE

Included in this month's solutions are thermal cameras, audio devices, facial recognition, and more.

#701

Access Control

Johnson Controls introduced the Tyco Illustra Insight, a facial recognition camera that allows authorized personnel to pass through an access control point without disrupting the flow of people. It does not require physical contact with a credential reader or keypad. Powered by artificial intelligence and deep learning algorithms, the camera leverages access control management software to simultaneously recognize multiple people. Integrated LEDs and audible messaging inform people whether they are authorized to enter an area.

www.illustracameras.com/insight



#702

Temperature Screening

FLIR Systems announced the FLIR Elara FR-345-EST, a fixed-mount radiometric thermal security camera that measures elevated skin temperature without contact or the need for a reference temperature source. Applicable for high-traffic airports, stadiums, commercial buildings, and manufacturing facilities, the camera automatically focuses on the body part that most closely correlates to core body temperature, accurate within 0.5 degrees Celsius, while maintaining social distancing guidelines. Whether used as a standalone system or integrated into a broader system, the camera's improved AI capabilities mean a faster assessment time, with an average of one second per person.

www.flir.com/fr-345-est



#703

Guard Station

Aiphone introduced the new IXG-MK IP Video Guard Station for screening visitors and improving security measures for multitenant and commercial spaces. The solution allows visitors to call a building's concierge, receptionist, or security guard directly from an entrance. Once safe intent is determined, calls can be transferred to the appropriate unit or the door can be unlocked for deliveries. A seven-inch touchscreen allows for clear video, and the station enables communication between guard stations, call recording, and call forwarding to tenants. The IXG-MK can have up to 9,999 units in its address book and maintains a history of calls received.

www.aiphone.com/video





#704 Body Cameras

Panasonic I-PRO Sensing Solutions Corporation introduced the BWC4000, a body-worn camera that offers law enforcement a solution with a 12-hour field-swappable battery. Other features include the ability to tag videos with metadata with a user-friendly LCD menu; MP4 file recording; H.264/H.265 video compression to maximize recording capacity; and 1080p, 720p, or 360p HD resolution in either a 16:9 or 4:3 ratio. Able to be used even in harsh conditions, the BWC4000 was built to meet MIL-STD 810H military testing standard with an IP67 weather-resistant rating. The new camera also offers built-in GPS, Wi-Fi, and Bluetooth.

www.publicsafety.i-pro.com



#705 Facial Recognition

SAFR from RealNetworks, Inc., announced improved face detection and recognition accuracy for both masked and unmasked faces with the release of SAFR 3.0. The latest version introduces a new default high sensitivity face detector, which boasts a 95.1 percent detection rate and 98.85 percent recognition accuracy rate for faces covered by PPE face masks—including non-surgical fabric masks of varying patterns—in surveillance-style videos of faces in motion. Detection efficiency was also improved when multiple faces are simultaneously in the field of view to ensure detection and recognition speeds remain high.

www.safr.com



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

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

CIRCLE #	PAGE #
08	Ameristar19
02	AXIS Communications04
07	CEIA Ferromagnetic15
01	ESRI.....02-03
10	Garret Metal Detectors25
05	Hanwha Techwin11
11	John Jay Online37
12	Mission 500.....43
13	Par-Kut International.....47
14	Prosegur.....67
06	Special Response Corporation13
04	Speco Technologies08
15	StarLink Fire LTE/Napco.....68
03	Zbeta Consulting06

advertisers online

Ameristar

www.ameristarsecurity.com

AXIS Communications

www.axis-communications.com

CEIA Ferromagnetic

www.ceia-fmd.com

esri

www.goesri.com

Hanwha Techwin

www.hanwhasecurity.com

Garrett Metal Detectors

www.garrett.com

John Jay Online

www.johnjayonline.com

Mission 500

www.mission500.org

Par-Kut International

www.parkut.com

Prosegur

www.prosegur.us

Special Response Corporation

www.specialresponse.com

Speco Technologies

www.specotech.com

StarLink Fire LTE/Napco

www.starlinklte.com

Zbeta Consulting

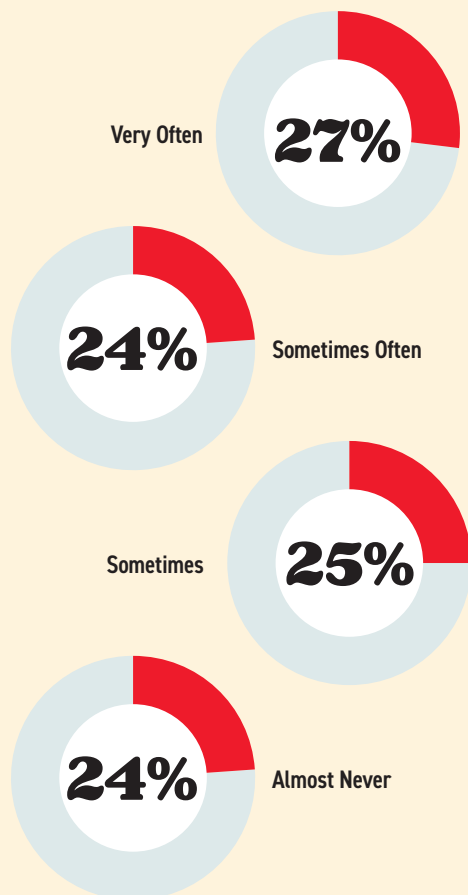
www.zbeta.com





Climbing Concerns

More than half of 1,500 Asian Americans who responded to an *AAPI Data 2020 Asian American Voter Survey* said they are worried about experiencing hate crimes, harassment, or discrimination because of anti-Asian rhetoric about COVID-19.



Hateful Backlash

At the beginning of the COVID-19 pandemic, the FBI warned that it expected a surge in hate crimes against people of Asian descent. While it is difficult to quantify the exact number of hate incidents because they often go unreported, advocacy group Stop AAPI Hate received more than 3,795 firsthand accounts of anti-Asian hate incidents in the United States between 19 March 2020 and 28 February 2021.

Despite Lockdowns, Hate Persisted

The Center for the Study of Hate and Extremism at California State University found that anti-Asian hate crimes spiked 149 percent across 16 of America's largest cities between 2019 and 2020, while reported hate crimes overall declined 7 percent during lockdowns and COVID-19 restrictions.

149%

Motivation Categories

There were 7,103 single-bias hate crime incidents reported in the United States in 2019, according to the FBI. Among those incidents, the motivations cited were primarily race or ethnicity. While anti-Asian hate crimes declined in the late 1990s, they have been on the rise in recent years.



Source: 2019 FBI Hate Crime Statistics

Hate Incidents Against Asian Americans and Pacific Islanders (AAPI)

According to Stop AAPI Hate, most reported incidents involved verbal harassment. More than 35 percent of discrimination incidents occurred at businesses, and race was cited as the primary reason for discrimination.



Verbal Harassment
68.1%



Physical Assault
11.1%



Online Harassment
6.8%



Shunning or Avoidance
20.5%



Coughed At/Spit Upon
7.2%



Workplace Discrimination
4.5%



You Now Have a New Choice in Security. 40 Years New.

Since 1976 Prosegur has deployed thousands of security guards around the globe. And installed countless security systems, including intrusion, video and access control.

We launched security operations centers, risk mitigation plans, cyber defenses and innovative security technologies for some of the largest companies in the world.

Our 160,000 employees are ready to help strengthen your organization's security, simplify its management and reduce its cost. To learn how, visit our website or call us today.



PROSEGUR
SECURITY

(888) 808-6992
www.prosegur.us


For product info #14 securitymgmt.hotims.com



Don't Wait Until It's Too Late

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



 **AT&T®** or **verizon®**

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

**StarLink Fire**

1.800.645.9445 • www.StarLinkLTE.com

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