SECURITY
MANAGEMENT

March/April 2022

Published by ASIS International

The Next ESRM Revolution

Advanced technology poses big challenges and bigger opportunities for strategic risk management.

By Val LeTellier

24/7
SEGUR
GUR

VISIT US AT ISC WEST
BOOTH 13114

It's your space.

Make sure you know when someone invades it.

SNEAK DETECTION

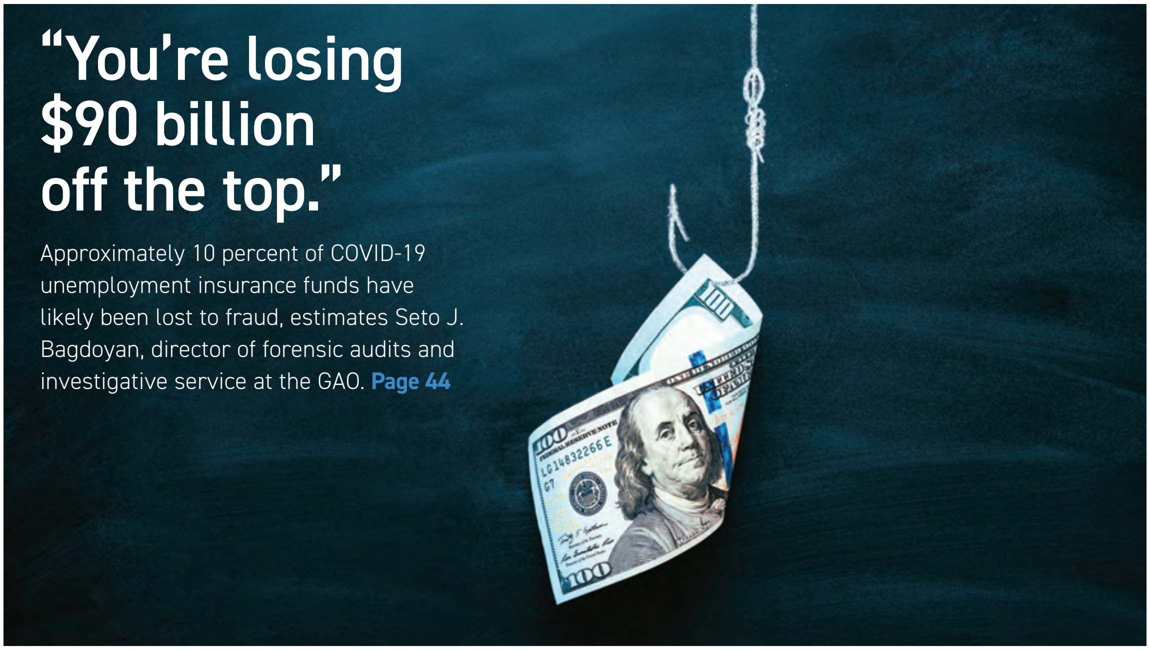
Our tailgate detection solution allows only one authorized person at a time. Its sleek design reduces cost and complexity versus mantraps and other devices, or it can even enhance those solutions. Your access control, made more secure—that's the Detex effect.

Call 800-729-3839 detex.com/sneak35

DETEX®

For product info #3 securitymgmt.hotims.com

Contents Notable



“You’re losing $90 billion off the top.”

Approximately 10 percent of COVID-19 unemployment insurance funds have likely been lost to fraud, estimates Seto J. Bagdoyan, director of forensic audits and investigative service at the GAO. **Page 44**

“Even though the CISO may be the leader of the security organization, they are not the only ones making security decisions at the organization.”

Sam Olyaei, research director at Gartner, explains how leaders must shift security conversations from controls to facilitation to keep up in modern enterprises. **Page 18**

77

The percentage of package theft victims who complain to the retailer, seemingly holding the company responsible for the loss. **Page 37**

$500,000

The reported cost per target device in 2016 to use Pegasus spyware from NSO Group. This prices out most law enforcement agencies, but some intelligence agencies can pay up to surveil dissidents and political targets. **Page 26**

“Data is the new oil.”

Val LeTellier cites Clive Humby to explore how emerging technologies and the data they generate can fuel enterprise security risk management strategies. **Page 33**

86

The percentage of the global automotive market consisting of connected vehicles by 2025. While these computers on wheels add advanced safety features, they are also at risk for cyberattacks. **Page 47**

Security Management (ISSN 0145-9406) Volume 66, Number 2, 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 © 2022 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.

ROBOT
AXIS

Contents Features

MARCH/APRIL 2022

EXECUTIVE TEAM

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

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

Nello Caramat
publisher
Nello.Caramat@asisonline.org

ASIS INTERNATIONAL

1625 Prince Street
Alexandria, VA 22314
703.519.6200
fax 703.519.6299

MEDIA SALES

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

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

Cover illustration by Stephanie Dalton Cowen

DOUBLE-PLAY COMBO!

FLEXIBLE PoE SOLUTIONS – by ALTRONIX

Deploy two security devices with a single cable, ensuring all your bases are covered.

▸ **NetWay3012P – PoE Adapter/Converter**
- Provides PoE+ (30W) and 12VDC simultaneously
- Supports IP cameras, external microphones, IR illuminators and more...
- Powered via PoE

▸ **NetWay2ES – 2-Port PoE+ Splitter**
- Provides PoE+ over 2-ports (60W)
- Supports IP cameras, illuminators, access devices and more...
- Powered via PoE

Altronix®

YOUR LEADER IN **POWER & DATA TRANSMISSION**

For product info #5 securitymgmt.hotims.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

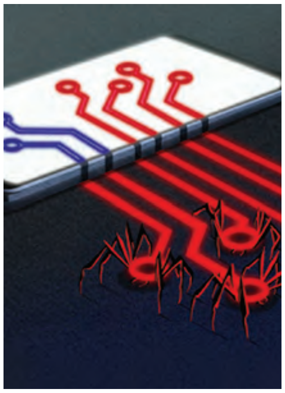
Caitlin Donohue
assistant art director
Caitlin.Donohue@asisonline.org

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.



Contributing Authors

Val LeTellier

FOUNDER | 4THGEN

Val LeTellier is a former U.S. State Department Diplomatic Security Service special agent and Central Intelligence Agency case officer. He is a member of the ASIS International Defense & Intelligence Community and National Capital Chapter. LeTellier leads 4thGen, a solutions-oriented consultancy enabling organizations to harness advancing technologies for greater efficiency, effectiveness, and mission success.

“The Next ESRM Revolution,” Page 28

Ben Stickle

ASSOCIATE PROFESSOR | MIDDLE TENNESSEE STATE UNIVERSITY

Ben Stickle is an associate professor of criminal justice at Middle Tennessee State University. He is a recognized expert in last mile delivery, focusing on package theft. His work has been featured in *AARP, Business Insider,* “Good Morning America,” *Loss Prevention Magazine, Mail and Express Review,* and many others.

“Pirates on the Porch,” Page 34

Michael Gips, CPP

PRINCIPAL | GLOBAL INSIGHTS IN PROFESSIONAL SECURITY

Michael Gips, CPP, is principal of Global Insights in Professional Security. He is an ASIS International member with more than 25 years of security experience, including as the association’s chief knowledge and learning officer and as an editor of *Security Management*.

Book Review, Page 17

Ben Rothke, CISSP, CISM, CISA

SENIOR INFORMATION SECURITY MANAGER | TAPAD

Ben Rothke, CISSP, CISM, CISA, is a New York City-based senior information security manager with Tapad with more than 20 years of industry experience in information systems security and privacy. His areas of expertise are in risk management and mitigation, security and privacy regulatory issues, design and implementation of systems security, encryption, cryptography, and security policy development. Rothke wrote *Computer Security—20 Things Every Employee Should Know.*

Book Review, Page 24

R. Scott Decker

FBI SPECIAL AGENT (RETIRED)

R. Scott Decker, PhD, is a retired FBI special agent with experience in violent crime, terrorism, and physical security. His book, *Recounting the Anthrax Attacks: Terror, the Amerithrax Task Force, and the Evolution of Forensics in the FBI,* won awards for nonfiction, true crime, and science and technology.

Book Review, Page 51

Hanwha
Techwin

It's time to eXpect more from your surveillance solutions

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

- **Unparalleled Image Quality**
- **Next-level cybersecurity**
- **Unprecedented Object Detection**

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

That's the power of Wisenet AI.

HanwhaSecurity.com

©2022 Hanwha Techwin America

ISC WEST

Visit us at Booth #14079

For product info #6 securitymgmt.hotims.com

Online Exclusives

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

Three Security Disconnects that Fall Through the Cracks

By Vanessa Dobrick

When there are unmitigated inconsistencies within an organization's security management system, it could effectively appear that the right hand doesn't know what the left is doing. When planning for a return-to-work environment, these discrepancies can present significant risk—as well as pose an economic impact—and they need to be overcome before the remote work evolution ends in a corporate dissolution.

In strengthening one's organization to withstand the challenges of tomorrow, it is critical to focus on the three most common disconnects taking place today around standardization, personnel, and system maintenance.

Addressing Mail-Borne Threats at Remote and Traditional Offices

By Will Plummer

In the last three years, the U.S. Postal Inspection Service and the U.S. Bureau of Alcohol, Tobacco, Firearms, and Explosives responded to an average of more than 10 dangerous mail or package incidents per day. Yet, most companies prioritize cybersecurity over threats posed by such attacks.

New solutions are emerging, and there is growing awareness of the problem, driven by recent high-profile mail threats against U.S. National Institute of Allergy and Infectious Diseases Director Dr. Anthony Fauci and the AstraZeneca COVID-19 vaccine plant. However, the challenge is growing, too. The shift in work routines—between work from home, hybrid, and return-to-office—presents more openings for attackers to exploit.

Companies should take precautions to keep employees and top executives safe from malicious mail and package threats, wherever they are working.

The Bull and Millionaire Mike

By Marie-Helen Maras, Jana Arsovska, and Kenji Logie

Academic research and media coverage of darknet marketplaces have predominately focused on cryptocurrencies, the sale of illegal drugs, firearms, stolen data (e.g., personal, financial, and medical information), counterfeit money and goods, child sexual exploitation material, and malware.

A crime not commonly associated with the darknet is securities fraud—a criminal offense under 18 U.S. Code § 1348, which involves the use of deceptive practices to influence or manipulate financial markets and/or others' financial investment decisions. Nevertheless, two recent criminal cases drew attention to the use of the darknet to commit securities fraud—Apostolos Trovias ("The Bull") and James Roland Jones ("Millionaire Mike").

In Case of Crisis, Build Community

By Sara Mosqueda

For an organization looking to prove itself resilient to a natural disaster, the planning phase must take into account steps well before an event blips on a radar—as well as look beyond its own walls.

After a weather event, one key element to consider while planning for recovery and getting back to speed sooner is coordination with the local community. While threats from inside or external attackers might target a specific business or person, a climate event doesn't differentiate between one building and another, much less one person and another. The value in having previously connected and developed a positive relationship with other community stakeholders—including churches, first responders, community centers, and utilities—is that this network can assist in a speedier recovery.

Photo by iStock, Illustrations by *Security Management;* iStock

Robbed in a Flash

By John Philippi, CPP, PSP

The heists have been brazen, fast, and organized. On 26 November 2021 alone, a crew of eight stole $400 worth of sledgehammers, crowbars, and hammers from a California Home Depot; a group pillaged a Bottega Veneta boutique in Los Angeles; and 30 people looted a Best Buy in Minnesota, grabbing armfuls of electronics, according to *The Washington Post*.

Flash robs—also known as multiple offender crimes, organized retail crimes, or flash mob robberies—involve large groups of people participating in a "smash and grab" theft in retail stores during business hours.

The increased frequency of flash robs could be attributed to a myriad of reasons, including overwhelmed police departments, reductions in criminal penalties as a result of criminal justice reforms, and overburdened prosecutors unable or unwilling to make such crimes a priority.

Trends in Theft, Training, and Terrorism

Hosted by Chuck Harold

John Philippi, CPP, PSP, joins the SM Highlights podcast to discuss flash robberies and their connection to organized retail crime. Also in this episode, sponsored by HID Global, learn how Michael Gips, CPP, and his synagogue committee retrained after a hostage incident in Texas, and Joshua Sinai explores the threat of edged weapon attacks worldwide.

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

TRENDING News & Analysis

Security Training

A rabbi held hostage for hours in a Texas synagogue attributed his escape to security training courses.

Tenuous Trust

Most people now distrust information until they see evidence that it is true, according to the *2022 Edelman Trust Barometer.*

Extremism in the Military

The U.S. Department of Defense updated its guidelines on handling extremism within its ranks, clarifying prohibited behavior.

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

SOCIAL MEDIA

KEEP IN TOUCH

@SecMgmtMag

@SecMgmtMag

ASIS International

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

MINDING THE METERS

In July 1935, newspaper owner Carl C. Magee installed 200 Park-O-Meters in the U.S. state of Oklahoma. The first parking meters in the world, they lined a busy commercial street in Oklahoma City and required $0.05 to park for 15 minutes to an hour, depending on the location.

Angry citizens immediately filed lawsuits in response, objecting to the meters' aesthetics and alleging that the city was fleecing motorists, *The New York Times* reported.

However, the responses from the public were not entirely negative. "In favor of the meters," the *Times* reported, "it is argued that shoppers and others visiting downtown buildings do not waste time when they think of the moving arrow checking off the passage of time. They get their business done as quickly as possible, hurry back to their cars and drive home, thus removing their automobiles from busy streets."

Through artificial intelligence, smart cities are able to gather real-time traffic data to better understand the movement of cars and figure out solutions to congestion.

The same basic balance is sought globally around parking today. In the United States, "250 million cars have an estimated 2 billion parking spots and spend 95 percent of their time parked," writes Dayna Evans in *Bloomberg Businessweek*. Reforms to parking include suggestions that cities "price street parking according to market value, based on the desirability of the space, the time of day, and the number of open spots."

Parking has become a science: balancing the cost of parking and the accessibility of spaces to provide a happy medium where consumers gain access to businesses but don't stay too long. But to find that equilibrium, cities require data.

Enter smart parking, which is projected to reach $19.29 billion by 2028, according to a recent report. This market, in turn, relies on data collection, analysis, and artificial intelligence (AI). According to *Parking Today*, "as cities strive to become smarter and more sustainable, artificial intelligence and its broad applications have been invaluable… Through artificial intelligence, smart cities are able to gather real-time traffic data to better understand the movement of cars and figure out solutions to congestion. This information can be used to recommend nearby parking spaces to cars in search of parking."

The revolution that took parking from the meter to the smart city has happened in numerous industries, including security. In this month's cover story, "The Next ESRM Revolution," Val LeTellier discusses the various data sources that "monitor, track, and assess behavior in real time." This "ubiquitous and persistent surveillance combined with advanced analytics has created a whole new enterprise risk equation."

These new data sets have benefits, according to LeTellier, helping to meet the goals of enterprise security risk management (ESRM) by "providing the predictive analytics to make security smarter, efficient, and proactive."

However, security professionals should be mindful of the pitfalls as well. "Data can be maliciously altered, advanced analytics can be inaccurate and even biased, and big data can create even bigger cybersecurity risks," he writes.

But, like smart meters—and the Park-O-Meter before them—big data and AI are here to stay. Learning to manage these new risks is security's next challenge. ■

Teresa Anderson

Teresa Anderson
Editor-in-Chief

Illustration by *Security Management;* iStock

A CAMERA WITH BARK AND BITE!

DON'T JUST WITNESS A CRIME. PREVENT IT!

LOUD AUDIBLE MESSAGE

Built-in speaker emits a siren and custom or preset warning messages.

BRIGHT VISUAL DETERRENCE

High-powered Blue and Red flashing lights trigger a flight response and draws attention to the scene.

"THIS IS A PRIVATE AREA!"

NDAA COMPLIANT

O4BDD1M

4MP IP Bullet Camera with AI and Audio & Visual Digital Deterrent® with Junction Box,
2.8-12mm motorized lens, white housing

NDAA COMPLIANT

O4TDD1M

4MP IP Turret Camera with AI and Audio & Visual Digital Deterrent® with Junction Box,
2.8-12mm motorized lens, white housing

Features

- Speaker with preset and custom sounds provide audio deterrence
- High-power red and blue lights provide visual deterrence
- Line crossing, object detection, region intrusion and video blurring detection
- People/Vehicle detection
- 2-way audio with talk-back feature enables voice communication through the built-in speaker

YEAR 5 WARRANTY

Call us at 1.800.645.5516 to learn more!

*Products are in compliance with NDAA Section 889 Part B Guidelines

FOLLOW US AT
SpecoTechnologies

speco® technologies

For product info #8 securitymgmt.hotims.com

A Tactical Adjustment

As security's profile changes within the company—from the frontlines to the boardroom—CSOs and CISOs must adjust their focus from tactics to value.

By Claire Meyer

Illustration by *Security Management;* iStock

Remote work is hugely popular with large swaths of the workforce. Many organizations find that this new arrangement results in higher productivity. According to research on remote workers from May 2020 through March 2021, nearly six out of 10 said they were more productive working remotely than they expected to be, and 40 percent said they were more productive than they were in the office. Large swaths of workers who said they could get their jobs done at home noted that they would like to continue to work remotely at least part time.

But remote work significantly impacted security measures. The perimeter spread from one campus to thousands of individual homes, intellectual property is now accessed via home Internet routers, and layers of carefully constructed security controls had to be bypassed to enable work to continue off-premises.

It's no longer about managing controls, it's about facilitation.

"That forced executives to say 'Well, why did we have those in the first place,'" says Sam Olyaei, research director for Gartner's Security and Risk Management Group. "'How can we secure an environment when it's no longer one office but it's now 3,000 offices because 3,000 people work in different environments?'"

Like the COVID-19 pandemic accelerated digital transformation and remote work adoption, the past two years have heightened the need for security leaders—CSOs, CISOs, and risk managers overall—to shift their position within the company to add and communicate value.

"That forced the CISO role to change—it's no longer about managing controls, it's about facilitation," Olyaei says. "It's coming to the point where the role of the CISO is more of a governance role than a technology role."

This shift requires a change in critical thinking and prioritization, both from the security leader and the organization at large.

"Security and risk management (SRM) leaders are being squeezed between an increasingly aggressive threat environment and the unrealistic expectation that the chief information security officer won't ever interfere with business unit computing," according to Gartner's report *Leadership Vision for 2022: Top 3 Strategic Priorities for Security and Risk Management Leaders*. "Successful CISOs recognize these misconceptions and actively work to change them in 2022 and beyond."

For example, the report said organizational leaders may believe that the CISO is onboard just to prevent breaches. Instead, the CISO should try to reframe that misconception—that the security leader is here to facilitate risk management.

"In general, you can certainly see a shift away from the tactical relationship that used to exist, where security would go to the business and talk about technology and projects," Olyaei says. "We're seeing that shift more towards it being a value conversation, where really the executives are less interested in the technology and the controls that the organization has and are more interested in the type of value that brings to the organization."

Part of that shift is a matter of influencing perceptions, reframing security as a value generator and competitive advantage—not a cost center. The other part of it is more challenging, Olyaei says. The new perception of security requires the personality and skill set to match.

It would be challenging for someone who came up the ranks of the IT function to be tapped as a CISO by default, he says, because he or she may not have the business experience to succeed in the current environment.

"Every organization requires a certain type of CISO," Olyaei continues. "That's why you see a lot of CISOs struggle when they get a higher paying job in a different industry. If a CISO from a large bank moves to a healthcare organization, well, the requirements are completely different, and the cultures are completely different."

Gartner conducted an in-depth analysis of 129 CISOs for its *CISO Effectiveness Index* in early 2020, measuring security leaders against four key areas: functional leadership, information security service delivery, scaled governance, and enterprise responsiveness. Only 12 percent of CISOs surveyed excelled in all four categories, with many allocating more resources and time toward tactical activities than they would like. The index noted that the emergence of COVID-19 only exacerbated the need for CISOs to focus on agility and strategy.

Researchers found that the top third of CISOs adopted five game-changing behaviors that differentiated high performers from the rest of the pack. The most effective CISOs initiated discussions on evolving norms to keep ahead of threats; prioritized keeping decision makers aware of current and emerging risks to the enterprise; proactively engaged in securing emerging technologies; formalized an actionable succession plan; and defined risk appetite through collaboration with senior business decision makers.

Book Review

Intimate Partner Violence, Risk, and Security

Edited by Kate Fitz-Gibbon, Sandra Walklate, Jude McCulloch, and JaneMaree Maher. Routledge; routledge.com; 284 pages; $39.96.

Home confinement during the coronavirus pandemic has increased instances of domestic violence around the world. UN Women, a group organized by the United Nations, calls violence against women a "shadow pandemic." According to the National Commission on COVID-19 and Criminal Justice (NCCCJ), violence against women has increased by 8.1 percent in the United States. But the estimates are much higher in other regions, including Colombia (up 175 percent), and Jingzhou, China (up 300 percent).

Routledge Studies in Crime, Security and Justice
INTIMATE PARTNER VIOLENCE, RISK AND SECURITY
SECURING WOMEN'S LIVES IN A GLOBAL WORLD
Edited by
Kate Fitz-Gibbon, Sandra Walklate, Jude McCulloch and JaneMaree Maher

Though it was published prior to the COVID-19 pandemic, the collection of research studies contained in *Intimate Partner Violence, Risk, and Security* explores intimate partner violence, particularly against women, as a global issue. Through a feminist lens, the authors effectively argue that gender violence is treated as a second-tier problem, beneath national imperatives such as terrorism prevention and response. As four of the authors conclude in the introduction, "Despite decades of feminist intervention on questions of violence against women, women's security remains marginalized."

The chapters fall into three categories: challenges in the contemporary global policy framework; national security, difference, and precarity; and everyday security and criminal justice questions. The section on criminal justice questions holds the most use for security practitioners, to assist in understanding context and environment, as opposed to practical advice or operational value.

Probably the most relevant research comes from the chapter "Domestic Violence Protection Orders and their Role in Ensuring Personal Security." To fulfill duty of care obligations or otherwise, companies sometimes assist staff in obtaining such orders against abusive spouses or partners. While the chapter doesn't delve into how companies can assist or the consequences of doing so, it sheds light on the efficacy of these interventions.

Another chapter seeks to establish a connection between climate change and intimate partner violence. The author points out that most of the world's farmers are women, and climate change is forcing them to become migrants—who are particularly vulnerable to partner violence.

Overall, this compilation is a scholarly review of domestic violence from a feminist perspective. It packs intellectual heft and would be a great resource for academics, researchers, sociologists, and intellectuals interested in criminal justice, women's studies, and violence. For the security practitioner, the work may be enlightening but lacks practical value.

Reviewer: Michael Gips, CPP, is principal of Global Insights in Professional Security. He has been in the security field for more than 25 years, including as an editor of Security Management *and chief knowledge and learning Officer at ASIS, where he remains a member.*

The last area—defined risk appetite with the appropriate stakeholders—requires significant soft skills and communication, Olyaei says. The security leader needs to be able to communicate the value of security at the board level, identifying emerging risks and explaining that it is okay to accept a certain level of risk—provided it is being monitored.

But Gartner analysis in its *Leadership Vision for 2022* report shows that nearly a quarter of directors are dissatisfied with the quality of current cyber risk information that management provides them. So, the appetite for frequent and thorough briefings is present from business units to the boardroom.

There are, however, some unrealistic expectations from stakeholders. The *Leadership Vision for 2022* report noted that one in five workers consider themselves digital technology experts since the beginning of COVID-19, but their consumer IT experience may not translate to enterprise security practicalities. It is up to the security risk management leader to align culture, communications, and future talent recruitment initiatives to bridge those gaps in understanding at all levels of the organization.

We can't expect our CISO to really be a chief or a C-level executive if they're still dealing with vendors and contracts.

Gartner set three levels of relationship priorities for security and risk managers: table stakes (working with the CIO, head of applications, head of infrastructure, and head of project management); value-building (connecting with the CEO, head of sales, communications leader, chief financial officer, and others); and differentiators. The latter category reaches primarily client-facing roles, including business unit leaders, chief marketing officers, and boards of directors.

"Building relationships with business unit heads, heads of sales, and heads of marketing is key as these are the exact areas where increased technology use is leading to a higher volume and variety of information risk decisions," the report said.

"Even though the CISO may be the leader of the security organization, they are not the only ones making security decisions at the organization," Olyaei adds.

HR directors are making purchasing decisions around remote work tools, product developers are building digital services and tools, and marketing teams leverage data analytics to gain insights on customer behavior. While the CISO may not control these decisions, he or she can influence stakeholders to consider security issues and benefits.

In addition, Olyaei says boards are more engaged and aware on cyber issues than ever. Olyaei adds that when he presents to the board, he prepares a 10- to 15-minute presentation to leave room for at least 40 minutes of questions and discussion. In years past, that ratio of presentation to discussion time was reversed. As a result of the increased attention, security leaders need to be prepared to field a variety of questions around strategy, emerging threats, and how security initiatives can empower the business.

All this cross-organizational interfacing takes time, however, and even effective security leaders do not spend as much time as they want on strategic planning and building relationships. According to Gartner's research, CISOs overinvest an average of 1.5 hours per week on security operations, followed by 1.2 hours on low-level staff management tasks. By contrast, CISOs underinvest two hours per week on stakeholder relationship-building, and they lag even further behind on strategic planning.

To free up security leaders' time, Olyaei suggests automating repetitive tasks like monitoring for alerts or log reviews to enable entry-level employees to take some tactical tasks off managers' plates. CISOs can also tap task captains to take charge of certain activities, such as contract management.

"These types of things are not what's going to create value for the organization, but rather it's the strategy side—interpersonal relationship building, the political dynamics of the organization," he adds. "We can't expect our CISO to really be a chief or a C-level executive if they're still dealing with vendors and contracts."

Violence Prevention in the Digital Dimension

Internet usage increased between 50 and 70 percent during the COVID-19 pandemic. Rates of cyber harassment and digital violence against women rose with it, including body shaming, cyber-flashing (sending unsolicited sexual images online), and doxing (sharing someone's personal information without consent).

One in 10 women in the European Union reported experiencing cyber-harassment—including receiving an unwanted or offensive sexually explicit email or text message or inappropriate or offensive advances on social networking sites—at least once since the age of 15, according to a United Nations fact sheet. Women between the ages of 18 and 29 have the highest rates of digital abuse. In the United States, two out of every 10 women in this age group said they had been sexually harassed online.

Cyber harassment and digital violence are factors in domestic abuse cases, as well. According to UK charity Women's Aid, 45 percent of domestic violence victims experienced some form of online abuse during their relationship, and 48 percent reported harassment or abuse online after the relationship ended.

Additionally, research from UN Women found that "The increasing reach of the Internet, the rapid spread of mobile information, and the widespread use of social media, especially since the onset of the COVID-19 [pandemic], and coupled with existing prevalence of violence against women and girls, have most likely further impacted the prevalence rates" of violence facilitated by information and communications technology.

Online violence results in higher levels of anxiety, stress disorders, depression, trauma, panic attacks, loss of self-esteem, and a sense of powerlessness to respond to abuse. As a result of experiencing violence online, many women restrict their use of digital services and products to avoid risk or revictimization.

In response to these findings and rising rates of online violence, the Council of Europe's Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO) released in November 2021 its first recommendations on the digital dimension of violence against women.

The document outlines the problem of violence against women committed online and enabled through different technologies, including stalkerware or spouseware tools that can spy on peoples' private lives through their devices without their knowledge or consent.

"For many years now, women's and girls' experiences of gender-based violence against women in these and other settings have been amplified or facilitated by technology, in particular the technology used in online and digital environments," the GREVIO recommendation said. "Information and communication technology (ICT) has enabled the perpetration of violence against women on a scale previously unknown. The onset of the COVID-19 pandemic in 2020 has further amplified this."

Growing Concerns

When asked how they feel about the outlook for the world, a majority of people said they were concerned.

😥 **23%** Worried

😟 **61%** Concerned

😊 **12%** Positive

😆 **4%** Optimistic

Source: *The Global Risks Report 2022*, World Economic Forum, January 2022

GREVIO's recommendations follow the four pillars of the Istanbul Convention—a 2017 Council of Europe Convention on violence against women—prevention, protection, prosecution, and coordinated policies, to identify next steps.

Overall, GREVIO recommends that countries and stakeholders review relevant legislation to take the digital dimension of abuse into account; undertake initiatives to eradicate gender stereotypes and discrimination; and promote the inclusion of digital literacy and online safety at all levels of education (people with lower digital proficiency are more likely to be victims of abuse).

GREVIO also suggested stakeholders make support services and counselling available to all victims; provide training and resources to specialists and telephone hotlines; equip law enforcement with the necessary tools and knowledge to investigate and prosecute online violence; and ensure the publication of incident reports by the criminal justice system. Stakeholders should include the digital dimension of violence against women in national strategies and action plans; establish systems to collect data on these incidents; and ensure data on suicide and gender-based killings contain accurate and relevant information on online harassment.

GREVIO also recommended that Internet providers and intermediaries be incentivized to moderate content and share responsibility to put an end to impunity for digital acts of violence.

As of *Security Management's* press time, the recommendations have not been formally followed by any countries. ■

Illustration by iStock

Installing a Legacy

All leaders want to make a mark on their organization. One healthcare system's security director wants his to be a long-lasting investment in surveillance.

By Sara Mosqueda

Not only was I concerned about someone just walking in the building, it was that they had access to everything.

The Riverside Health System operates four acute care hospitals, two specialty hospitals, six nursing home facilities, and one behavioral health hospital throughout the coastal Virginia region. Across its facilities, more than 600 clinical providers and 9,500 team members help provide medical care for roughly 2 million people every year.

When Darryl Ware became the director of the Riverside Safety and Protection Department in 1997, he cast an eye on revamping the organization's surveillance system—knowing full well it would be a larger project.

Ware, who comes from a law enforcement background, understood that hospitals and medical facilities face a unique and fluid threat environment. His leading concern was that the majority of threats to hospital facilities, staff, patients, and visitors had shifted from infant abductions to workplace violence, theft, and others.

In the late 1990s, Riverside maintained an open-door policy. "You could literally walk in the front door of any hospital," Ware says. He wanted to immediately change the set up and compartmentalize parts of the hospital to make it harder for a threat actor to get into any or all areas. "Not only was I concerned about someone just walking in the building, it was that they had access to everything," Ware recalls.

Some changes included increased access control components, especially between entrances and other more sensitive areas, such as medicine closets, newborn nurseries, and hot labs—laboratories that handle and host radioactive medicines for tests and other medical procedures.

But by 2010, Riverside had reached the limit of what it could accomplish with its existing security system—a blend of elements such as older surveillance cameras and newer additions like staff badges. Ware realized that the solution needed here was not simply newer systems, but adaptive ones that could change with the times and the threats.

The previous cameras the hospital used were similar in style to the "old behemoth prison cameras that you see in Burt Reynolds movies," Ware says, and they stuck in his mind as he began searching for a video management system (VMS). Adaptability was what he wanted from a VMS—not only an ability to play well with security solutions and tools from other manufacturers and developers, but the system needed to also serve as the foundation for the evolution of Riverside's security.

Photo courtesy of Riverside Health System

Once you're able to convince the C-suite and they get on board, they will usually stay on board, especially if you can keep things flat.

Ware ultimately landed on Genetec's Omnicast VMS because it offered a centralized approach to the technology portion of its security detail. First installed between 2012 and 2013, Omnicast allowed Ware and the protection department to monitor, track, and operate access control functions and manage video feeds.

When Ware's team decided it was finally time to upgrade the analog behemoths to digital cameras, Omnicast provided a key advantage. Since different cameras could be integrated onto the platform, it afforded the department a chance to consider a wider range of different models and manufacturers.

"I considered it a legacy system," Ware says, but not because it seemed dated or old to him. Instead, Ware adds, he classified it this way because it would leave a long-lasting mark on the hospital system's security program.

Ware was given the chance in 2020 to update the old, large format surveillance cameras installed along the hallways of Riverside facilities.

Working with his integrator, Ware chose Axis Communications surveillance cameras and received information and specialized training on using the cameras and their various capabilities. Riverside leadership supported the proposal, and the organization began replacing the older cameras.

But for Ware, one of the best features is that the cameras can connect and coordinate with Omnicast. The platform, which is an IP-based VMS, allowed Riverside's security department to organize the cameras, each one with a unique identifier that indicates its location within a facility to keep feeds organized.

When he was first looking at Omnicast, Ware knew that the system would be able to integrate with smartphones and other mobile devices. Given the organization's budget constraints, however, these were features that were brought on later—once they became more affordable.

Ware says that the VMS put "the infrastructure in place that I needed—a camera system that I could manage, (covering) well over 186 buildings, spread out over 400 square miles. I could sit in my office and if someone said, 'Hey, we had a break in last night,' I didn't have to get in my car and travel." Now, Ware can review the incident and coordinate a response from his computer or smart device.

The newer cameras garnered enough support from both the security department and the C-suite that the organization approved installing IP-based cameras in future facilities.

Another useful benefit of the Omnicast system may initially appear prosaic: timestamps. But Ware is fond of them when reviewing video feeds related to incidents of stolen property or missing pharmaceuticals. The timestamps generated by the VMS help Ware and his team determine who was in the area or room when an item was taken, and security is usually able to identify the thief or thieves using the video feeds.

The feeds' timestamp function is also helpful in more commonplace instances, such as keeping security staff accountable. Some areas in Riverside's facilities are sensitive, remote, or require additional security for other reasons. Omnicast links up with installed access card readers to track guard tours, ensuring that these areas are frequently patrolled—in line with the organization's policies. As they patrol, guards scan their ID cards at readers, which serve as checkpoints. With Omnicast programmed to track the check-ins, Ware can generate a monthly report with data that can help benchmark his department's effectiveness.

The cameras also cover the healthcare facilities' parking garages. For one employee, this helped identify an ex-boyfriend who damaged her vehicle while she was working.

The cameras recorded the man driving into the garage, and motion sensing features—which are part of the surveillance software—kept track of him as he exited his truck, crawled underneath two other cars, and slashed all four tires of the employee's vehicle.

"We were able to get that information to the police prior to the team member getting off work and discovering all of this," Ware says.

While the Omnicast VMS and security department were unable to prevent the damage to the car, the tools and team together played a key part in preventing the man from directly confronting and possibly harming the employee.

Ware plans to continue branching this system out and connecting with future security solutions. One upcoming project is an entrance weapons detection solution, which Ware says he is confident will have the backing of the C-suite since the newer solution with Omnicast will operate as a crime deterrent and keep attack statistics steady.

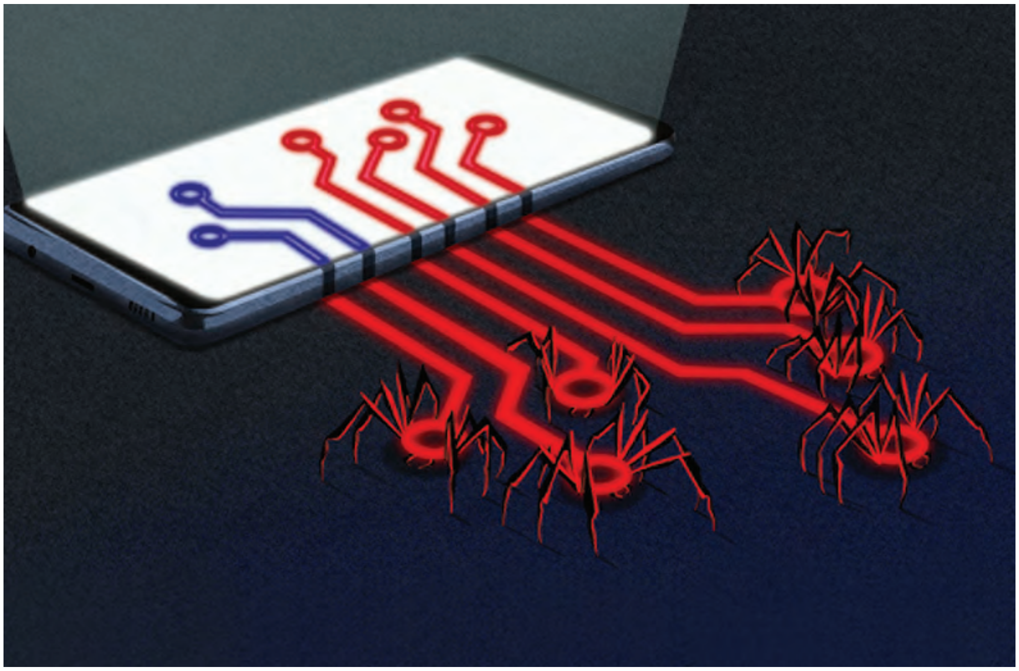
"Once you're able to convince the C-suite and they get on board, they usually will stay on board, especially if you can keep things flat," Ware says. ■

For more information, contact Genetec's Mark Feider, *mfeider@genetec.com*

Dual-Use Dangers

Interception and intrusion cyber capabilities sold by private companies are increasingly being marketed to intelligence and government agencies. New efforts attempt to stop them from winding up in the hands of U.S. and NATO adversaries.

By Megan Gates



The military and intelligence agencies have deeper pockets than the police.

It's not typically seen as an act of defiance. But when Loujain Alhathloul got behind the wheel in 2014, that's exactly what it was. She pledged to drive from the United Arab Emirates (UAE) into the Kingdom of Saudi Arabia in protest of the kingdom's ban on women driving.

Alhathloul had moved back to Saudi Arabia in 2013 after studying at the University of British Columbia. During her time in Canada, Alhathloul expressed her opinion that the Saudi driving ban should be lifted, her sister told NPR. So, she moved back to the kingdom to put some horsepower behind her words.

Alhathloul made it to the border before being detained and imprisoned for 73 days. The incident, however, did not dissuade her. Alhathloul continued her activism before being arrested by kingdom authorities again in 2018, just days before the country lifted the prohibition on women driving. But this time she would be accused of passing information to journalists and foreign diplomats, as well as attempting to change the Saudi legal system, and she was sentenced to five years and eight months in prison for violations of the kingdom's counterterrorism law.

In May 2021, under pressure from the United States to review relations in response to its human rights record, Saudi Arabia released Alhathloul from prison. In December 2021, the Electronic Frontier Foundation (EFF) filed a lawsuit in the U.S. District Court of Oregon, Portland Division, on her behalf against software maker DarkMatter Group and three of its former executives for hacking Alhathloul's iPhone to track her communications and whereabouts, information that was passed on to the UAE security services. (*Loujain Hathloul Alhathloul v. DarkMatter Group, et al.,* U.S. Dist. Ct. of Oregon, No. 3:21-cv-01787-IM, 2021)

Providing this information to the UAE allegedly led to Alhathloul's detainment, imprisonment, and torture in Saudi Arabia. The lawsuit also claimed that Alhathloul continues to have severe restrictions on her freedom of movement, in violation of her fundamental rights.

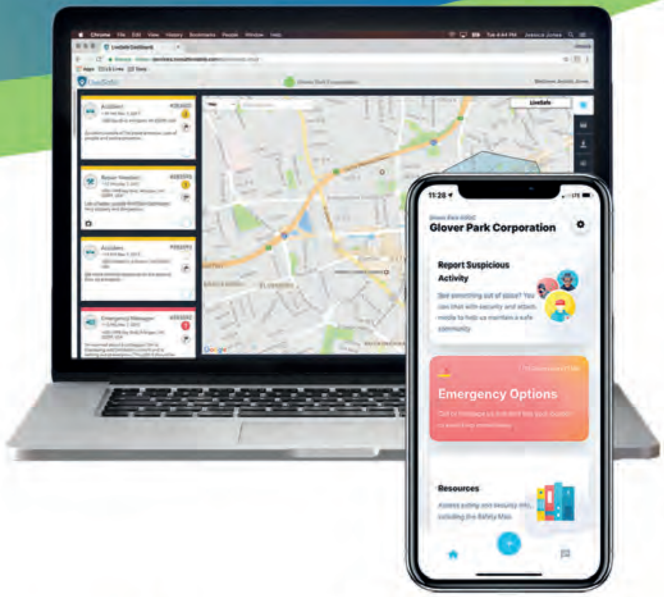
"No government or individual should tolerate the misuse of spy malware to deter human rights or endanger the voice of the human conscious," Alhathloul said in a statement. "This is why I have chosen to stand up for our collective right to remain safe online and limit government-backed cyber abuses of power."

The lawsuit is just one of a variety of actions and efforts that came to fruition in 2021 to provide

Illustration by Sara Gironi Carnevale

The Top Solutions for Security, Risk Management and Safety Professionals

Empower and Protect your Organization with the Leading Platforms for Risk and EHS Management and Safety Communications for Everyday or Urgent Scenarios



Vector LiveSafe™

Identify safety and security threats, send emergency notifications, and engage employees with two-way safety communications.

Vector EHS Management™

Conduct risk assessments, identify controls, and remediate hazards.

VectorSolutions.com/RiskManagement

VectorSolutions™

For product info #11 securitymgmt.hotims.com

When these firms begin to sell their wares to both NATO members and adversaries, it should provoke national security concerns.

more insight and accountability for how cyber capabilities—including interception and intrusion capability technologies—are being sold by private companies and used by public sector actors.

The market for these technologies has grown considerably, with an increasing number of vendors selling to law enforcement, governments, and intelligence services. While some of these vendors act responsibly, others are selling their products to actors that could use them to harm the vendor's home country or private citizens.

Recent research published by the Atlantic Council's Scowcroft Center for Strategy and Security highlighted this dichotomy. It found that multiple firms in Europe and the Middle East are marketing cyber interception and intrusion capabilities to U.S. and North Atlantic Treaty Organization (NATO) adversaries.

"The authors found that 75 percent of companies likely selling interception/intrusion technologies have marketed these capabilities to governments outside their home continent," according to *Surveillance Technology at the Fair: Proliferation of Cyber Capabilities in International Arms Markets*. "Five irresponsible proliferators—BTT, Cellebrite, Micro Systemation AB, Verint, and VASTech—have marketed their capabilities to U.S./NATO adversaries in the last 10 years."

To make those conclusions, the researchers analyzed exhibitor lists for ISS World Training, a trade show for lawful interception and intrusion products, cross referenced with research by the Omega Research Foundation's Arms Fair database, says Johann Ole Willers, a PhD fellow at the Copenhagen Business School and a co-author of the Atlantic Council research.

The researchers looked at vendors' attendance at ISS World and various arms fairs, along with their product offerings and the location of the arms fairs where vendors advertised relative to their headquarters. The researchers used this process to identify marketing practices, not actual sales, Willers adds.

They then confirmed with "high confidence" that at least 59 companies are "highly likely to market interception/intrusion technologies at any arms fair they attend," according to the paper. "Some of the companies (like Croatia's Pro4Sec and India's ClearTrail) advertise lawful interception services on their websites for military, law enforcement, and intelligence agency clients. Others (like Italy's Area s.p.a and Germany's Wolf Intelligence) have vague websites or no websites at all, but have been called out by news media for selling interception/intrusion tools."

Micro Systemation AB (MSAB) CEO Joel Bollö says he has not read the Atlantic Council report fully, but he denies that the company is an irresponsible proliferator and that it has marketed its products to U.S./NATO adversaries.

"We sell to law enforcement, not to military regimes," he adds, explaining that as a Swedish company, MSAB follows Swedish export control laws for selling its products, including mobile forensics software for timely access.

Bollö says that MSAB sells its products only to government entities and countries permitted by the European Union, including those in Australia, Japan, North America, and Singapore, that have a legal right to access devices—

Book Review

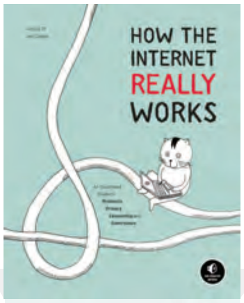
How the Internet Really Works

By ARTICLE 19. No Starch Press; nostarch.com; 120 pages; $19.95.

It wasn't that long ago that a car manual was 100 pages or shorter. Today, they can be close to 700 pages long. As cars get more complicated, so do the manuals. And so does the driver's confusion when he or she must figure out how to get a new computer on wheels to operate.

When it comes to the Internet, its manuals are known as RFCs (Request for Comments). In the early days, one could be familiar with the entire family of RFCs. As of this review, there are more than 9,000 RFCs, which means the complexity is such that a single person simply cannot know everything about how the Internet operates.

But in a nutshell, how does the Internet work? In *How the Internet Really Works: An Illustrated Guide to Protocols, Privacy, Censorship, and Governance* (No Starch Press), the reader gets a short, interesting, and entertaining overview of the Internet without having to read all the RFCs.



The listed author of the book is ARTICLE 19, an international non-profit organization that aims to promote, develop, and protect freedom of expression, including access to information. As such, much of the book has a focus on security and privacy. While ARTICLE 19 is the official author, one of the contributors is Mallory Knodel, chief technology officer for the Center for Democracy and Technology, who brings her extensive security and privacy expertise to the written word.

With electronic censorship so rampant across the world, the book provides readers with an understanding of how security and privacy work on the Internet, from the transport layer of how data moves to the protocols that perform those functions and more. By having this understanding, a person can better ensure their security and privacy is safeguarded, rather than just taking someone's word for it.

For those looking to understand how the Internet works, but in a jargon-free style that will educate them and not confuse them further, *How the Internet Really Works* is the book for them.

Reviewer: Ben Rothke, CISSP, CISM, CISA, is a New York City-based senior information security manager with Tapad and has more than 20 years of industry experience in information systems security and privacy. His areas of expertise are in risk management and mitigation, security and privacy regulatory issues, design and implementation of systems security, encryption, cryptography and security policy development. Rothke wrote Computer Security – 20 Things Every Employee Should Know.

MADE IN THE USA
LIFETIME WARRANTY

such as if law enforcement seizes a suspect's phone during an investigation.

MSAB has also voluntarily withdrawn its business from certain regions and can take measures to blacklist its technology should the company become aware that it is in the hands of an unauthorized user.

For instance, Bollö says that MSAB withdrew its business from Hong Kong after the British ceded control of the region to China and the People's Republic of China began to overhaul Hong Kong's democratic practices.

"In Hong Kong, a regime shifted fast, and we can't go in and bring back our tools—that's not something we can do," Bollö says. "But what we can do is we can make sure that the product cannot be updated. It won't work anymore. And we can blacklist it, so if software comes from somewhere else it will make it impossible to work with that device as well."

Three of the other named actors in the report, BTT, Cellebrite, and VASTech, did not return requests for comment. A spokesperson for Verint said that in 2021, the company split to form a sister company—Cognyte—which is the focus of the report and that Verint is not involved. Cognyte did not return requests for comment.

The reasons why the market for these tools has grown vary, but Willers says it is partially in response to rising costs associated with them and a shift away from law enforcement customers to government agencies and intelligence firms.

"Law enforcement has a problem of finding the money to buy these products, so naturally, as a company capable of delivering them, they would turn elsewhere," Willers adds. "The military and intelligence agencies have deeper pockets than the police."

For example, NSO Group's Pegasus spyware was reportedly sold for $500,000 per target device in 2016. That's too expensive for many law enforcement agencies with tighter purse strings, Willers explains, so companies seek out other clients.

Many companies would consider these alternative customers legitimate, but the researchers highlighted that when "these firms begin to sell their wares to both NATO members and adversaries, it should provoke national security concerns for all customers."

For instance, in September 2021, the U.S. Department of Justice (DOJ) entered a deferred prosecution agreement with three former U.S. intelligence community and military personnel—the same executives named in Alhathloul's suit—who worked as senior managers for a UAE-based company to carry out hacking operations for the UAE government between 2016 and 2019, a violation of the International Traffic in Arms Regulations.

"These services included the provision of support, direction, and supervision in the creation of sophisticated 'zero-click' computer hacking and intelligence gathering systems—i.e., one that could compromise a device without any action by the target," the DOJ said. The company "employees whose activities were supervised by and known to the defendants thereafter leveraged these zero-click exploits to illegally obtain and use access credentials for online accounts issued by U.S. companies, and to obtain unauthorized access to computers, like mobile phones, around the world, including in the United States."

Instances like this point to a problem of an unregulated and unclear marketplace for intrusions, the authors of the Atlantic Council report explained.

"While offensive cyber capabilities are helpful for law enforcement and border protection, the dual-use nature of many of these capabilities provides opportunity for malicious employment as well, especially when the capabilities are sold to authoritarian actors," they wrote.

To help curb this activity, Willers and his co-authors—Winnona DeSombre and Lars Gjesvik—said more research needs to be done on the marketplace, especially on Chinese vendors' activities. They also recommended companies implement know-your-customer policies, that arms fairs limit irresponsible proliferators' attendance at events, tightening of export-control loopholes, and naming and shaming irresponsible vendors and customers.

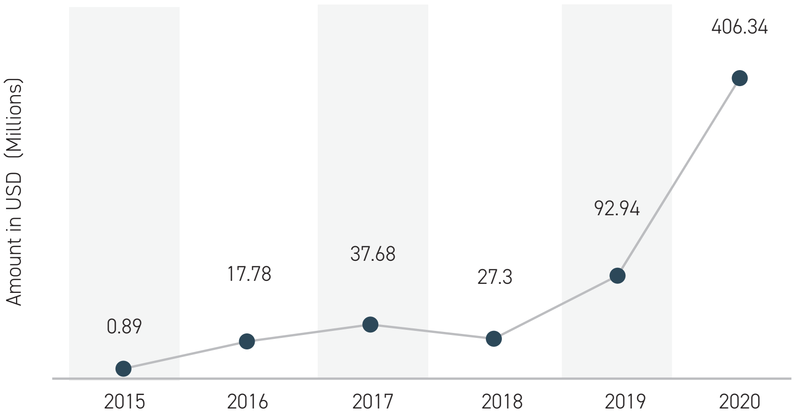
Action on some of these fronts is already happening and is encouraging, Willers says. For instance, in May 2021 the European Union approved its long-awaited Dual-Use Regulation that created new rules for cyber surveillance technology and export restrictions based on public security and human rights considerations. The regulation went into effect on 9 September 2021 and shows that the EU is formally detailing that "if you sell these products, then certain rules apply," Willers says.

The United States is using a slightly different approach—what Willers describes as more akin to a "large hammer"—to send a "strong signal immediately" that certain activity will not be tolerated.

On 3 November 2021, the U.S. Commerce Department's Bureau of Industry and Security added Israel's NSO Group to its Entity List for developing and supplying spyware to foreign governments that used the technology to target academics, activists, businesspeople, embassy workers, government workers, and journalists. Organizations on the Entity List are prohibited from exporting, re-exporting, or conducting in-country transfers of items—including technology—that pose a significant risk to the national security or foreign policy interests of the United States.

The Extortion Economy

Cryptocurrency payments to ransomware actors' addresses increased drastically between 2015 and 2020.



Source: *The Global Risks Report 2022*, World Economic Forum, January 2022

The bureau said in a press release that these tools allowed foreign governments to conduct transnational repression to silence dissenters beyond their borders, threatening rules-based international order.

"The United States is committed to aggressively using export controls to hold companies accountable that develop, traffic, or use technologies to conduct malicious activities that threaten the cybersecurity of members of civil society, dissidents, government officials, and organizations here and abroad," said U.S. Secretary of Commerce Gina M. Raimondo.

75 percent of companies likely selling interception/intrusion technologies have marketed these capabilities to governments outside their home continent.

The U.S. Office of the Director of National Intelligence, along with the U.S. State Department, also issued a consumer guide on how to protect themselves from commercial surveillance tools.

And that's not the only action against NSO Group. In November 2021, Apple filed a lawsuit against NSO Group and its parent company to hold it accountable for surveilling and targeting Apple users with its Pegasus spyware.

"State-sponsored actors like the NSO Group spend millions of dollars on sophisticated surveillance technologies without effective accountability. That needs to change," said Craig Federighi, Apple's senior vice president of software engineering, in a statement. "Apple devices are the most secure consumer hardware on the market—but private companies developing state-sponsored spyware have become even more dangerous."

Apple's suit seeks a permanent injunction to ban NSO Group from using any of the company's software, services, or devices.

Ultimately, Willers says there is no perfect solution to this problem because the industry will continue to exist. The important thing, he says, is "to define what is acceptable and what is not."

The naming and shaming that has been targeted towards NSO Group has worked to some extent, Willers says. The U.S. government placed the company on its Entity List, and Israel also moved to limit the number of countries its companies can export products to.

"The big surprise will be if it is enough to draw a red line for other market actors," Willers says. "There are other companies out there that might not be as big...but they're not doing fundamentally different stuff."

NSO Group did not return a request for comment on this story. DarkMatter could not be reached for this story. ■

The Next ESRM Revolution

The applications and implications of advanced technology signal big changes for risk management. Security leaders need to be alert to adopt the right technology that enables the enterprise to weather future hurdles.

By Val LeTellier

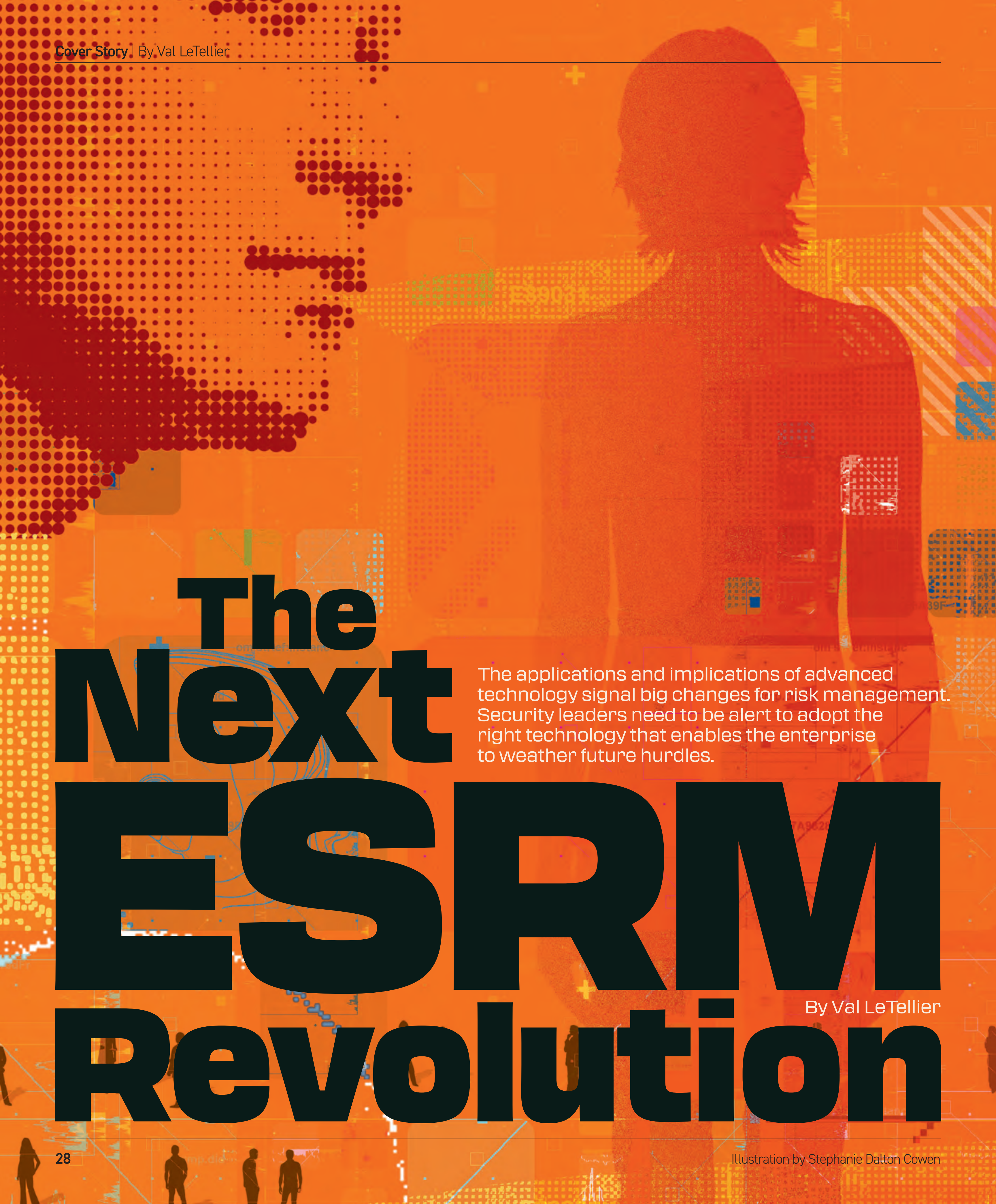


Illustration by Stephanie Dalton Cowen

Cover Story | By Val LeTellier

The Fourth Industrial Revolution is here.

We live and work in an interconnected world in which machines, devices, sensors, and people connect and communicate with each other. We are surrounded by smartphones, Internet of Things (IoT) devices, location detection technologies, advanced human–machine interfaces, cyber–physical systems, cloud computing, authentication tools, fraud detection measures, smart sensors, advanced analytics capabilities, and digital customer profiling. Smart cities are coming online, with operators able to access enormous sets of information to manage systems.

These technologies are transforming the global industrial landscape, and they are changing enterprise security risk management (ESRM) in ways the security industry is only starting to understand.

Klaus Schwab of the World Economic Forum predicted that the Fourth Industrial Revolution would bring about the "fusion of our physical, our digital, and our biological identities." For security leaders, this fusion is important—it enables multiple surveillance surfaces to monitor, track, and assess behavior in real time.

The result: Ubiquitous and persistent surveillance combined with advanced analytics has created a whole new enterprise risk equation.

New Technologies, New Possibilities

In today's digital world, there is an exponentially growing array of digital sensors that collect massive data pools of information—much of it on individuals and their activities. With the advent of robust data analytics, this bulk information can be enriched by other data sources to create valuable intelligence for risk mitigation and incident investigation.

Some of this data is volunteered by individuals through their use of technology. For example, Facebook boasts more than 2 billion active users per month; its subsidiary Instagram has 800 million monthly users; and Twitter claims more than 330 million monthly active users. All of these users generate data.

In other instances, providers of technology and services collect personal data from consumers and users. Surveillance capitalism in the form of ad-tech sensors collect and track shopping and purchasing behavior, with the data sold to commercial data consumers. Cellular phone networks, DNA mapping, and virus tracking add to the mix. Technological advances like high-speed and high-density 5G cellular networks, ubiquitous IoT infrastructures, and vehicle telemetry provide refined triangulation of an individual's movement.

Other data comes through different channels. One of every two adult Americans are in a law enforcement face recognition network, according to the Georgetown Law Center on Privacy and Technology. The U.S. Government Accountability Office (GAO) has also identified 16 U.S. states that let the FBI use face recognition technology to compare the faces of suspected criminals to driver's license and ID photos.

While these massive data lakes were nominally valuable, it took improvements in data analytics to really make them useful. Machine learning (ML) and artificial intelligence (AI) enabled the aggregation of data sets, the correlation of activity, and real-time and forensic exposure of events.

Fusion technologies have further empowered data analytics by eliminating the spaces between data points and connecting dots that once took days or weeks to link—if they could be connected at all. The fusion is created by a suite of algorithms that churn through public and proprietary records, live sensor feeds, and surveillance archives to identify patterns and connections and allow analysts to draw direct lines between incidents and individuals.

Long gone are the days when people could exist most of the day offline. Now, it's rare to find moments when people are beyond the reach of the sensors surrounding them. The implication of this technological data empowerment is significant for government and corporate security officials; new mechanisms and methodologies are now available to identify and mitigate risk.

A notable example is the FBI investigation into the 6 January 2021 riots at the U.S. Capitol. Federal charging documents show that advanced technologies were employed to identify and prosecute suspects by correlating video surveillance records, facial and gait recognition, license plate readers, cellphone tracking, and online communications. Federal prosecutors have said the investigation is likely to be "one of the largest in American history, both in terms of the number of defendants prosecuted and the nature and volume of the evidence."

According to Chuck Wexler, executive director of the Police Executive Research Forum, "If the event happened 20 years ago, it would have been 100 times harder to identify these people, but today it's almost impossible not to leave your footprints somewhere."

Even at the security officer level, there are bespoke applications that enable the monitoring, tracking, and reporting of suspicious activity through real-time streaming of video surveillance feeds. Silicon Valley firm Knightscope, for example, takes this a step further by eliminating the human sensor completely, equipping autonomous security robots with license plate readers, thermal heat sensors, and facial recognition capabilities. Instead, humans are relied on to respond to alerts from the robotic and autonomous sensors.

While near or actual real-time correlation is a game-changer, so is the more nuanced execution of deep dive investigations that find patterns in unstructured data compiled over years and decades through phone, financial, and travel records. To a high degree, technology is dramatically streamlining the investigatory grunt work expended in complex investigations.

Government and corporate security leaders are finding themselves in a complex environment in which real-time and forensic investigations using ubiquitous sensors and advanced analytics are increasingly the norm, and they are realizing the possibilities, caveats, and dangers.

The Good

Arguably, the paramount goal in risk management is to prevent harmful incidents from occurring. Next generation security technology enables exactly that, providing the predictive analytics to make security smarter, efficient, and proactive.

For example, forensic and predictive security methodologies are created by applying advanced analytics to dissembled video surveillance data packets. Recent advancements in end-point computing allow ML and AI processing to be built into video surveillance systems for local execution of automated facial recognition, number plate recognition, patterns, and anomalies, transmitting finished analysis to security operating centers for action.

Technology has also streamlined the cooperation between security leaders and police. Beyond facilitating a quick response to incidents, advanced technology is now a core component of police investigations. Facial recognition helps track suspects, and location tracking leveraging mobile device usage makes it easier to correlate anomalies against technical surveillance. Video of criminal activity is often captured by witnesses or even the criminal themselves, which can then be corroborated by phone records, video surveillance, and personal statements. Such is the case of Matthew Perna, 37, who posted a detailed and lengthy social media video of himself at the U.S. Capitol on 6 January 2021. Within a year he pled guilty to obstruction of Congress, entering a restricted building without lawful authority, and disorderly conduct.

The Bad

No technology is without some drawbacks, particularly emerging and evolving technologies. Data can be maliciously altered, advanced analytics can be inaccurate and even biased, and big data can create even bigger cybersecurity risks.

While altered photos and deepfake videos are well-known, less is known about intentionally manipulated data sets that can often go unidentified and alter findings and conclusions. Machine learning and artificial intelligence are built upon algorithms and models created from sample data sets that may have unrecognized biases, such as facial recognition tools that are trained on predominantly Caucasian faces and are less reliable when detecting people of color.

Additionally, the more stored information an organization has, the greater a target it is for data theft or ransomware attacks. Because the data is often held by others (cloud providers), end users need assurances of security and privacy. Enterprise risk managers tend to rely upon their organization's IT department for this, but given the criticality of this role, it is worth understanding the experience and expertise of these stakeholders.

In addition to the technological risks, there are human resources risks in play. Pandemic-induced remote work will likely remain a big part of enterprise security's challenges. After a period in which business leaders have lost a direct view of their employees, many organizations moved toward digital surveillance to ensure productivity. But as firms adopted digital surveillance in the form of monitoring of email accounts, Web browsing, collaboration tools, and even webcams and keyloggers, many organizations are seeing increasing employee turnover due to potential privacy issues.

As reported in a 2021 VMware study *The Virtual Floorplan: New Rules for a New Era of Work*, approximately 40 percent of companies implementing device monitoring or planning to do so have witnessed either increased or drastically increased employee turnover.

The Ugly

While some employees respond to digital surveillance by finding a new job, others skirt official corporate networks, tools, and safeguards in favor of shadow IT.

The increased use of personal devices for work purposes to evade monitoring tools is rightfully concerning to risk managers, particularly as it is often accompanied by cutting corners and neglecting policies and procedures to save time and effort. A good example is forwarding sensitive data to a personal device or account so it can more easily be edited or printed. By doing so, that information then rests unprotected on a personal device and outside the organization's control—and maybe even outside the employee's control.

Best ESRM Practices

As illustrated above, advancing technologies and methodologies are dramatically changing the way the way we live, particularly in a COVID-19 era. But what does it mean for enterprise security and those who manage it? A lot, given that ESRM requires a holistic view of overall security risk and places the responsibility for security risk management decision-making with the asset owners.

Per ASIS International's guideline on ESRM, the concept sits atop four pillars: holistic risk management, stakeholder partnership, transparency, and governance. It is a risk-based approach to managing security programs based on the concept that you cannot protect what you do not understand. To address your organization's risk, you need to know its mission, needs, and priorities.

Next generation security technology is valuable for achieving ESRM precepts; it can be used to identify and prioritize assets, identify, and qualify risks to those assets and then determine the best way to mitigate those risks.

Holistic risk management. One of the best ways to consider all types of security risk is to make data work for you. Security tools are generating increasing amounts of data, so risk managers have a distinct advantage to transform their roles. Security leaders can better protect their infrastructure by identifying issues and security gaps before an incident occurs. They can leverage this data to become a more integral part of the organizational value chain by the way they collect, transmit, and analyze their data.

Fusion technologies allow risk managers to add new sources of data to correlation engines through new networks of sensors, further enabling organizational risk management, efficiency, and effectiveness—impacting the organization's bottom line.

For example, dashboards can be built to monitor sensors, alert, and then report indicators of potential problems. They can integrate disparate security devices and correlate their unstructured data into a single pane of glass that not only monitors and reports the health and performance of security infrastructure, but also the health and performance of the organization writ large. These software platforms combine security, safety, and productivity data to create a common operating picture that feeds business intelligence directly to the computers and mobile devices of enterprise leaders, enabling smarter decision-making, melding cross-organizational ESRM partnerships, and reinforcing the fact that secure facilities are critical to the organizational bottom line.

Stakeholder partnership. In the ESRM framework, security professionals are trusted partners who advise asset owners and work with others to define and enforce security policy. This approach naturally requires robust communication and data sharing with stakeholders. A game-changing solution to this challenge is harnessing the cloud.

Cloud services provide enterprise security risk managers a way to enhance transparency and accountability. Cloud services enable the uploading of massive data sets for analysis and real-time information sharing with risk stakeholders, allowing them—with the proper permissions and administrative roles—to see the same vulnerabilities, liabilities, and gaps that security managers are citing.

As noted above, applying predictive analytics and machine learning against surveillance data can be valuable to achieving non-security stakeholders' goals, such as enhancing productivity and performance. That said, the introduction of employee monitoring tools must be done in a way to maintain morale and avoid dangerous unintended consequences.

Transparency. Cloud services can enable transparency with stakeholders about the nature of identified risks and efforts to identify, prioritize, and mitigate them. That said, the challenge of leveraging advancing technology while protecting employee privacy is not minor. Monitoring of any type and level can generate the perception that employees are not trusted. As such, while transparency is important, so is trust.

The COVID-19 era has accelerated the move toward greater personal data collection. It also showcased how varied personal points of view can be on a single issue. Risk managers should keep these issues in mind when considering the advanced security technology needed and how to present it to stakeholders.

Transparency is critical to gaining buy-in and protecting privacy, as is evaluating deployment requirements, particularly if the organization is deploying a solution across multiple sites. Some transparency is often legally required, especially in countries under data governance regulations. Advanced analytics can transform business operations and streamline compliance, security, and control harmful events, but it's unlikely that everyone within the organization will singularly see it that way. Communication and outreach are vital.

Governance. ESRM governance should align with overall organizational governance, and a committee should lead risk tolerance discussions to make top-level decisions. Given that these decisions will undoubtably include complex issues like advanced technologies, employee privacy rights, and legal issues, security leaders may need to take the lead in educating the stakeholder team on relevant issues.

First though, enterprise security risk managers need to educate and involve themselves. They need to understand the value and risks that advancing technology brings to organization, in terms of risk identification, qualification, and mitigation, as well as in bottom-line productivity.

These technologies, methodologies, and cultural norms are complex and evolving quickly, so this is no easy task. Risk managers serve themselves well by taking time to stay current and informed.

Mapping the Revolution

Humans have always developed better technologies to help make life easier—upgrading from stone to bronze, from coal to electricity, from railroads to airplanes. As new devices, digital tools, and connectivity advance, academics and researchers see the dawn of the Fourth Industrial Revolution approaching. But how did we get here?

1765

First Industrial Revolution

- Mechanization
- Introduction of the steam engine
- Specialized manufacturing industries (steel, textiles, tools) established

1870

Second Industrial Revolution

- Electricity, gas, and oil
- Mass production scales up manufacturing and drives economies
- Introduction of the internal combustion engine
- Development of communications methods, including telephones

1969

Third Industrial Revolution

- Nuclear energy
- Rise of electronics, telecommunications, and computers
- Automation changes production lines
- Creation of the Internet
- Globalization connects markets and resources

Today

Fourth Industrial Revolution

- Physical–cyber systems
- Robotization
- Big data and analytics
- Artificial intelligence
- Virtual and augmented reality

Technology's ESRM Impact

In the right situation, technology can provide a competitive advantage. As business enablers, ESRM leaders can and should leverage specific aspects of the Fourth Industrial Revolution to help their organizations accomplish their missions. Pursuant to that, several themes stand out.

Data can make ESRM more empowered, efficient, and effective. As the saying goes, data is the new oil. The evolution of analytics has driven business leaders to lead and manage based upon data. If the data is accurate, it can enable informed decision-making—a good thing.

As a business enabler, ESRM needs to employ the same approach. Every access control, fire, and cyber–physical intrusion sensor shares data and builds an increasingly sophisticated and structured data set. This information is extremely valuable for enabling real-time risk mitigation but also identifying patterns and profiles to assess future situations, streamline processes, and reduce human effort.

Cloud-managed AI powered video surveillance systems, edge devices, and 5G networks are disrupting traditional surveillance systems with human analytics, face recognition, and behavioral analytics built directly into the camera using AI chipsets. This edge computing reduces the need for high bandwidth backhaul and storage, facilitating scalability and affordability. It also allows ESRM leaders to place and maintain more sensors, which in turn provides greater data for organizational risk and productivity assessment.

Organizational leadership sees these capabilities in everyday life, and naturally expects their application to security. The wide availability and affordability of advanced technologies once only accessible to wealthy firms has changed the landscape. Now, personal data, advanced analytics, facial recognition, and cloud computing are widely available either as licensed software or as a service.

At varying levels, employees understand what is within the realm of technological possibility because they see it in their daily lives through consumer devices, website tracking, and other services, and they expect to see it in the workplace.

Organizational leaders responsible for profitability have the same perspective, but with more of a focus on efficiency and cost-savings. They expect real-time accountability, which is rarely achievable without advanced technological underpinnings. They also want transparency and to be more involved in enterprise security, even to the point of receiving live feeds from surveillance cameras via smartphone apps to monitor business flows. And because they understand and use cloud computing in their job, they know they can affordably have the insights and accountability they are requesting.

Keeping pace with the rapid evolution and application of these technologies requires a significant dedication of time and effort. While daunting, keeping pace with the most significant advancements in intelligent surveillance, cloud services, and data correlation domains—at least at a high level—is worthwhile. Like in any marathon, once you get behind it's hard to catch up.

As an example, risk managers should understand that the future of video surveillance technology includes data analyzed on-site, reduced server costs, and improved functionality and efficiency enabled by high-bandwidth, high-density 5G networks.

Security risk managers should also understand the legal aspects of fusion technology. In the United States, there are no laws at the national level restricting the blending of data sets to generate information that would require a court order to obtain, but that could change to align with regulations like the EU's General Data Protection Regulation (GDPR). In the meantime, organizations must carefully consider the risk/gain equation of what technology they use and how they use it.

Effective data correlation is critical to the successful use of these technologies. The Fourth Industrial Revolution is creating data at an amazing speed. Every day in 2021, Internet users created 2.5 quintillion bytes of data—adding up to 79 zettabytes of total data created, captured, copied, and consumed globally. That's a huge leap from 15.5 zettabytes in 2015.

In the security world, enormous amounts of streaming data are being created by a wide range of monitoring and surveillance systems. Everything from cybersecurity monitoring, surveillance camera feeds, access control, vehicular reports, power usage/distribution, HVAC, and more are hitting security control centers simultaneously and without interruption.

Regrettably, much of this data is delivered in non-standardized and unstructured formats. So, the trick becomes finding the truly usable data points needed to connect for effective analysis.

Video surveillance is by far the greatest contributor to the security data challenge, particularly when the associated metadata is included. It's this metadata that enables algorithms to find anomalies and draw conclusions that people—and many computers—can't find on their own. It can even identify problems an enterprise may not even know it had.

The key is finding a way to better harness and understand this data for enterprise risk and operational security insight.

ESRM talent requirements have evolved. The experience and expertise required of enterprise risk managers have quickly evolved during the last two decades. At a minimum, managers must be appreciative of the value of technology as applied to threat reduction, security efficiency, and overall effectiveness. They must be tech-savvy, adaptable, and, in some cases, capable of managing a team that is able to fuse disparate data sources for analysis.

The ability to harness advancing technology is no longer a "nice to have" attribute of security professionals—now it's table stakes for entry and promotion.

The Fourth Industrial Revolution is underway. It is up to security and risk leaders to manage its applications to benefit the enterprise. Risk managers who know how—and when—to leverage new technologies will capture leadership roles as their contributions to the organization's big data transformation process positively impact risk management and productivity. ■

Val LeTellier is a former U.S. State Department Diplomatic Security Service special agent and Central Intelligence Agency case officer. He is a member of the ASIS International Defense & Intelligence Community and National Capital Chapter (NCC). LeTellier leads 4thGen, a solutions-oriented consultancy enabling organizations to harness advancing technologies for greater efficiency, effectiveness, and mission success.

PIRATES on the PORCH

Consumers are increasingly turning to home delivery. Savvy thieves are patrolling porches for packages to purloin. Retailers and delivery firms are taking the hit.

By Ben Stickle

E-commerce spiked during the COVID-19 pandemic, and it shows no sign of slowing down. Consumers ordered medicine, groceries, electronics, and more in record numbers as officials encouraged them to stay at home. Online shopping—especially when done from a mobile device or smartphone—has increased for consumers across the world, according to a September 2021 PricewaterhouseCoopers (PwC) survey.

"Forty-one percent of respondents say they shop daily or weekly via mobile or smartphone, compared with 39 percent six months ago and 12 percent five years ago," PwC reported in its December 2021 *Global Consumer Insights Pulse Survey*. "Only 6 percentage points separate mobile shopping from in-store shopping."

Packages were left at doorsteps, porches, and mailboxes daily—tempting so-called porch pirates to roam neighborhoods in search of goods to steal.

Package theft has emerged as one of the most common types of crime in the United States. This is not only aggravating for consumers, but it carries legitimate security and risk implications for any business seeking to safeguard the last few feet of its product's journey.

The theft occurs during the trip from the store to the consumer's doorstep, a distance often referred to as the last mile. Package theft is different from mail or cargo theft, however; the author and fellow researchers define it as "taking possession of a package or its contents, outside of a residence or business, where it has been commercially delivered or has been left for commercial pick-up, with intent to deprive the rightful owner of the contents."

While package theft and porch piracy are relatively new terms to the industry's lexicon, their impact on the retail sector is already notable. A 2016 study by smart door lock manufacturer August Homes found that nearly 11 million consumers were victims of package theft. A recent study by SafeWise estimated that 210 million packages were stolen in 2021. Assuming an average value of each package at $25, the impact of porch pirates in the United States in 2021 was more than $500 million.

With the spread of COVID-19, consumer habits dramatically shifted in early 2020—more people were purchasing items online that were then delivered to their homes, as reflected in the SafeWise study. The buy-online boom has somewhat slowed from its peak, yet it remains strong and likely signals a permanent shift in consumer behavior. It also means that, in some cases, the only physical interaction a consumer has with a retailer is at the doorstep.

As a result, there is another shift occurring, where traditional risks from retail shrink within brick-and-mortar stores are increasingly hitting home or arriving at consumers' porches. Porches are no longer solely an extension of a residence—they are now a commercial center, and thieves know it.

Methods of Marauding

Porch piracy has minimal risk for offenders and a low cost of entry—no special skills are required to carry off a box. In addition, significant social media coverage of package theft likely leads to greater awareness of new and effective techniques among criminals.

It is difficult to measure the full scope of package theft, however. Most U.S. states lack adequate laws addressing the theft of packages not delivered by the federal U.S. Postal Service (especially as many online commerce companies use non-government or contract delivery services), resulting in lax law enforcement and investigations.

Most victims of package theft do not report the incident to police or insurance providers, so these crimes are rarely officially recorded. Instead, victims most often turn to the retailer for refunds or replacement items, and—in most cases—merchants replace the item and take the loss without specifically identifying where the loss occurred in the last mile. Few, if any, retailers share data on losses from package theft, focusing instead on attempts to placate customers and protect brand reputation. The result is a perfect storm confronting retailers and consumers, making understanding the crime and enacting effective countermeasures difficult endeavors.

In some cases, the only physical interaction a consumer has with a retailer is at the doorstep.

The author and fellow researchers conducted a study, *Porch pirates: examining unattended package theft through crime script analysis*, in 2020, analyzing 67 YouTube videos of package thieves in action to gather data. They used their findings to create a Crime Script Analysis, which described porch pirates' actions, demographics, targets, and methods.

Pirates. There was a nearly even split on the gender of porch pirates, which is unusual for most crimes. Based on the video data, these offenders tended to be younger than 45 years of age (95 percent) and had a societally reflective distribution of race and ethnicity—54 percent were Caucasian, 15 percent Black, 9 percent Hispanic, and 3 percent Asian.

Very few pirates appeared to case the home (only 12 percent), and even fewer (8 percent) attempted to disguise their appearance during their actions. The use or appearance of gates, fences, cameras, and homeowners' cars did not appear to dissuade thieves. Most casually walked up to the doorstep (72 percent), did not attempt to see if anyone was home (73 percent), and subsequently ran away after picking up the package. More than 60 percent used a vehicle to escape—typically pulling right into a victim's driveway. Two-thirds of observed thieves (63 percent) had an accomplice, usually a driver.

Packages. The study also identified 98 packages stolen from residents, with most thefts occurring within 25 feet of a roadway (61 percent). Nearly all of these items were visible from the roadway (93 percent). Additionally, 46 percent of the stolen packages had a brand visible on the box, and nearly half of the packages were medium-sized—approximately 13 to 36 inches.

It was infrequent for a package to be opened on site, occurring in just 3 percent of cases. In only a few cases (10 percent), thieves made multiple trips onto the property to gather all the packages.

Everyone's a Loser

Package theft has been growing for years, with few concerted efforts to confront the issue. A retailer may view a package leaving its warehouse or store on a delivery truck as a completed sale. The delivery company leaves a package unattended outside a home, which transfers ownership to the intended recipient in most U.S. states. For the homeowner who never receives a stolen package, however, he or she is most likely to blame the retailer.

Ultimately, nearly everyone along this vertical loses. The consumer fails to receive the item promptly. Delivery services divert resources into investigating missing packages. The retailer must investigate losses and decide whether to replace items, bearing the cost of the stolen items and additional replacement shipping.

> Porches are no longer solely an extension of a residence—they are now a commercial center, and thieves know it.

While retailers and delivery services may not be liable for the theft, they are carrying the brunt of the impact. Fifty-two percent of respondents who previously identified as victims of package theft reported the theft to the shipping company, but 77 percent filed a complaint with the retailer, according to the 2019 survey *Fear of Package Theft: A Survey of Online Retail Customers*. Whether rightly or wrongly, victims of package theft seem to hold the retailer responsible for the loss.

Additionally, 34 percent of victims took steps to avoid future thefts, using methods including purchasing cameras and lockable package receptacles, or requesting delivery to an alternative address. Some went so far as to avoid buying expensive items online due to fear of theft (23 percent).

Beyond altering purchasing behavior, victims spurred by fear may shift to other retailers. These behaviors can severely impact retailers financially—companies that often already absorb the costs of replacing an item and risk losing future sales.

Retailers should consider the experience and safety at the customer's porch or front step in the same way they consider the customer experience at a traditional brick-and-mortar store.

Thankfully, this is beginning to occur on a broad scale. Companies are responding to package theft by implementing many techniques, including drone delivery, scheduled drop-offs, parcel lockers, delivery inside consumers' homes, and more. For example, Amazon offers customers the option to have their purchases delivered to a secure locker at nearby Whole Foods locations. Amazon also offers an in-home delivery service for customers whose homes utilize certain smart home features—within a delivery window, a driver can request to unlock a customer's door using an Amazon handheld scanner and, upon verification and while being monitored, the package can be left inside the building instead of on the front porch. The driver then exits, locks the door, and continues on his or her route.

The Last Foot

Recent consumer behavior indicates that home delivery is here for the long haul. The front porch, previously seen as mainly a facet of a neighborhood's social setting, has been stretched and shifted to include a crucial aspect of e-commerce. And due to shifts in criminal activity during the COVID-19 pandemic, package theft is likely to continue increasing in step with consumer buying trends.

Within the last mile is the most critical stage and one of the most vulnerable points of the entire supply chain—the last foot. This is the distance between where the package is left on the porch or doorstep to when it reaches the intended recipient's hands. Securing the last foot requires a combined effort between consumers, retailers, delivery services, and law enforcement.

The best way to tackle this problem that costs retail and consumers millions annually is to rethink the porch.

Retailers. Retailers must evaluate a loss occurring within the last mile to identify at which point in the supply chain that the package is stolen.

Using this information, they can partner with consumers to encourage or require appropriate responses, such as directing delivery to post office boxes or private lockers, pick-up drop-off (PUDO) locations, or purchasing delivery insurance.

Further, retailers should consider the risks of using packaging that reveals the box's contents—specific brands, logos, or products could attract thieves.

Who's Afraid of Porch Pirates?

Fear of package theft results in consumers changing their purchasing and delivery decisions, according to a 2019 survey of more than 500 people across the United States. The subsequent report, *Assessing the Fear of Package Theft* by Melody Hicks, Ben Stickle, and Joshua Harms, found that nearly 24 percent of participants had experienced package theft, but many more were concerned and adjusted behaviors accordingly.

27%	of survey participants said they were either "fairly" or "very worried" about package theft.
41%	got orders delivered to a different location to mitigate theft risks.
28%	had orders delivered on a specific day or time to prevent theft.
23%	avoided buying expensive items online because they were afraid their orders would be stolen.

Source: Assessing the Fear of Package Theft, *American Journal of Criminal Justice, 2021*

Packaging and shipping. Packaging companies can help mitigate package theft through a crime-conscious approach to readying an item for shipping. Reducing the size of a box, using muted or subdued colors, removing or covering any visible branding from a box, and using tamperproof tape are all tactics that can camouflage a package's contents.

Delivery companies can also take small—but meaningful—and targeted steps to reduce the likelihood of thefts. This includes notifying consumers when a package arrives, whether through an app, email, text, knocking on the door, or ringing the doorbell. Company instruction or training can direct delivery personnel to leave packages behind an item on the porch—such as planters or columns—which may reduce the package's visibility from the street. Packages with brands and lithium battery labels (which clue thieves to the contents) can be placed on a doorstep facedown, eliminating the label's visibility.

Consumers. Ideally, consumers should remove packages from the porch as soon as they are delivered. If someone is unable to do this, consider delivering a package to a trusted neighbor or a more secure location, such as an office building, a P.O. Box, a private locker, or a PUDO location. Other alternatives could include using a container like a home parcel locker placed on the porch that can house packages—useful if consumers live close to a roadway, in a high crime area, or frequently receive valuable items.

Police and government leaders. Currently, most U.S. states do not have sufficient laws aimed at combatting porch piracy, but updating or developing new legislation to track, report, deter, or appropriately penalize package theft could help.

Further, tracking thefts will allow for a more robust understanding of how, when, and where package theft occurs and which people or organizations are behind these crimes. Since package thefts often cluster in occurrence, prevention methods—such as coordination with neighborhood watch groups—and encouraging the use of social media to alert homeowners may be helpful. ■

Ben Stickle is an associate professor of criminal justice at Middle Tennessee State University. His work has been featured in *Mail and Express Review, Loss Prevention Magazine, Business Insider,* "Good Morning America," *The New York Times, AARP,* and many others.

WE ARE METRO ONE

METRO ONE LOSS PREVENTION SERVICES GROUP

If you are looking for world-class service, unparalleled integrity and ethics, and customized solutions, Metro One LPSG is your best and only choice for security and loss prevention services.

Established in 1984, Metro One LPSG has over thirty-seven years of experience and the cutting-edge technology necessary to elevate your security program to the highest level possible.

- Client-Dedicated Infrastructure
- Performance Driven
- Leaders in Account Management
- We are NOT for Sale
- Young Ownership
- Privately-Held

metroonelpsg.com

ISO 9001:2015 CERTIFIED COMPANY

PRI Registrar
PERFORMANCE REVIEW INSTITUTE

For product info #15 securitymgmt.hotims.com

Learn how Metro One can benefit you:
As a client: solutions@metroonelpsg.com 833.708.6800
As a career: talent@metroonelpsg.com metroonejobs.com

Illustration by *Security Management*; iStock

Haste Makes Waste

To fend off an economic crisis during the COVID-19 pandemic, the U.S. government pumped billions of dollars into emergency loan and unemployment insurance programs. Some of that money went to legitimate borrowers, but billions went to fraudsters. **By Megan Gates**

The COVID-19 pandemic put many businesses in a predicament. They needed to close their doors to stop the spread of the virus. But they also needed to make money to continue to exist and to pay their employees.

To help make up the difference, many business owners and operators applied for emergency loans that, if used appropriately, would be forgiven by the U.S. federal government.

That's the course James R. Stote, 55, and Phillip J. Augustin, 52, were on when they applied for a Paycheck Protection Program (PPP) loan in mid-2020 for Augustin's company, Clear Vision Music Group LLC. The PPP loan was guaranteed by the Small Business Administration (SBA) as part of COVID-19 relief efforts under the U.S. Coronavirus Aid, Relief, and Economic Security (CARES) Act.

There were just a few problems. Stote and Augustin falsified the documents to obtain the loan, and then after submitting an initial application, they worked to obtain even larger PPP loans for themselves and others. They used fake payroll numbers, false Internal Revenue Service (IRS) forms, and phony bank statements to submit for or facilitate at least 79 fraudulent loan applications worth at least $35 million.

One of those loan applications was for Diamond Blue Smith, 36, a recording artist and member of the rap group Pretty Ricky. Smith obtained a PPP loan worth $426,717 for his company, Throwbackjersey.com, using falsified documents. After receiving that initial loan, Smith reapplied for another PPP loan for his other company, Blue Star Records LLC—also with falsified documents. He received a loan of $708,065 and spent at least part of it at the Seminole Hard Rock Hotel and Casino and to purchase a Ferrari.

Smith's activity was ultimately noticed by law enforcement, which arrested him. While detained, Smith told investigators he paid Stote and Augustine at least $250,000 in kickbacks for their help in preparing and submitting the loan applications.

Augustin, Stote, and Smith all pled guilty to conspiracy to commit wire fraud and were ordered to pay more than $1 million each in restitution. Federal agents also seized the Ferrari.

This investigation marked a win for the authorities, but it exemplified a particularly pernicious problem. In the wake of the COVID-19 pandemic, fraudsters have eagerly taken advantage of government loan programs, supply chain disruptions, and a generally overwhelmed public.

Government Program Fraud

To help bolster the economy and boost aid for people impacted by the COVID-19 pandemic, financial firms and governments around the world released billions of dollars in the form of unemployment insurance, loans, and grants to stimulate their economies.

In the United States, the government took similar measures. The U.S. Congress passed the American Rescue Plan and the CARES Act, which made $2.2 trillion available in loans, grants, and payroll protection to keep businesses open and maintain household income.

Part of that effort was the PPP, which initially included—with subsequent expansions in 2020 and 2021—more than $814 billion in loans to provide incentives for businesses to keep workers on payroll or rehire laid-off workers. Individuals and businesses applied for PPP loans to SBA-approved lenders, credit unions, and financial technology companies. If loan holders abided by the rules for receiving the loan and used the funds appropriately, the loan would be forgiven.

Additionally, the SBA was tasked with overseeing the COVID-19 Economic Injury Disaster Loan (EIDL) program. This new program provided $154 billion in emergency low-interest loans to help cover operating and other expenses—of up to $2 million—for eligible U.S. small businesses.

To help ensure that the money allocated through these programs was used responsibly, Congress tasked the U.S. Government Accountability Office (GAO) with tracking how it was used and conducting audits of the SBA. The GAO has also been receiving reports about the programs via its FraudNet hotline—where anyone can report allegations of fraud, waste, abuse, or mismanagement of federal funds.

Howard Arp, director, forensic audits and investigative service, GAO, oversees the FraudNet hotline. During the last two years, he says approximately 40 percent of incoming complaints were related to the CARES Act. These range from false eligibility for relief programs, misuse of funds from relief programs, and even complaints from people who received a PPP loan but never applied for one.

"We document the complaint and then have it for future reference," Arp explains. "If the complaints are fairly specific, that instance and allegation of fraud is referred to the appropriate Office of Inspector General or the Department of Justice. We also have it documented, and we can consider it for future work and ongoing work."

Additionally, the GAO began reviewing the distribution process for PPP and EIDL loans, how loans are transitioned into forgiveness, and the reported risks and fraud associated with these stages.

"We also were seeing cross-cutting fraud, people were not siloed," says Rebecca Shea, director, forensic audits and investigative service, GAO. "People were exploiting the PPP and EIDL and then the tax credits as well, and unemployment insurance. We're starting to see an increasing number of cases that were exploiting programs…it could run the gamut…VA contract fraud to stealing checks out of people's mail for those tax credits."

The GAO made a series of recommendations to improve oversight of PPP and EIDL, some of which the SBA has acted on. In the meantime, however, the GAO has placed the emergency loan programs on its High-

Consumers in the Crosshairs

While COVID-19 fraud has broadly impacted governments and businesses, it is also impacting consumers. For instance, Canadians reported 29,590 instances of pandemic-related fraud between 6 March 2020 and 30 November 2021 to the Canadian Anti-Fraud Centre (CAFC).

The Anti-Fraud Centre is Canada's national repository for information on fraud, reporting fraud, and providing resources to identify it. It also provides information on fraud to law enforcement, including the Royal Canadian Mounted Police.

To find out how the COVID-19 pandemic has impacted the CAFC and the types of fraud reports the centre is receiving, *Security Management* spoke with Sue Labine, call centre operations supervisor in charge of the Fraud Intervention Intake Unit.

Labine's unit typically acts as the first point of contact for individuals who want to report an incident of fraud—either by phone or through an online reporting tool. The CAFC then validates those reports and provides support to victims.

Due to the increasing prevalence of fraud targeting older adults, the centre also has a Senior Support Unit that specializes in working with seniors—including connecting them with another individual who has been a victim of the same scam, Labine says.

Before the COVID-19 pandemic, the types of fraud in 2018 with the highest dollar losses reported to the CAFC were romance scams (CAD $22.5 million) and wire fraud (CAD $12.5 million). Loan (CAD $11.9 million), extortion (CAD $10.2 million), and investment (CAD $8.7 million) scams were also linked to high dollar losses in 2018.

"Victims are being told that they could invest into a fake company, but they think they're investing with a legitimate platform," Labine explains. "Returns are always extremely high and at the end when it comes to reclaiming their funds, there are barriers to getting their money back. They lose the majority of their investment."

Since the pandemic began, the CAFC has seen an uptick in investment scams. Between January 2021 and September 2021, 1,557 instances were reported for a total of CAD $70.2 million in losses.

The centre has also seen an increase of reports of phishing attempts and social engineering tactics leveraging COVID-19 related content. For instance, fraudsters sent emails about where to claim relief funds with a link ultimately used to steal someone's personal information to commit identity fraud, or they offered to sell lists of COVID-19 infected people in a specific neighborhood to steal financial data.

The CAFC has also received reports of fraudsters calling vic-

Risk List because SBA has not finalized plans to oversee its PPP and EIDL program, placing hundreds of millions of federal dollars at risk of improper payment. The GAO High-Risk List consists of U.S. federal programs and operations that are vulnerable to waste, fraud, abuse, and mismanagement, or programs that need broad reform.

“The Small Business Administration has provided hundreds of billions of dollars’ worth of loans and advances to help small businesses recover from adverse economic impacts created by COVID-19,” the GAO said in a release. “While loans have greatly aided many small businesses, evidence of fraud and significant program integrity risks need much greater oversight and management attention.”

SBA was caught by surprise in a variety of ways, but they could have been much better prepared.

Johana Ayers, managing director of forensic audits and investigative services at the GAO, says, “This area was added because there was a belief on our part at GAO that these programs, like the other issue areas, were at high risk for fraud, waste, and abuse, and were in need of significant transformation.”

The GAO based this assessment partially on the fact that SBA’s own independent financial statement auditor had noted in December 2020 that PPP loans and EIDLs went to “potentially ineligible borrowers,” according to a GAO report.

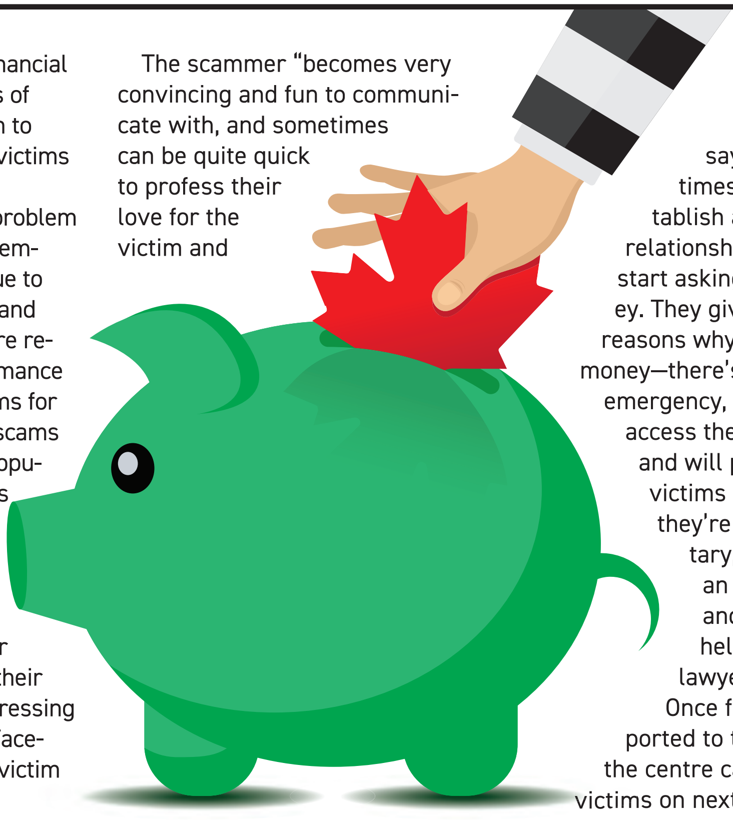
“For example, the auditor noted that there were over 2 million approved PPP loans (with an approximate total value of $189 billion) flagged by SBA that were potentially not in conformance with the CARES Act and related legislation,” the GAO explained. “The auditor also identified over 6,000 disbursed EIDLs (with a total value of over $212 million) that were issued to potentially ineligible borrowers.”

Additionally, financial institutions filed more than 21,000 and 20,000 suspicious activity reports related to PPP and EIDL with the Financial Crimes Enforcement Network (FinCEN) between May and October 2020, when funds became available. The SBA’s Office of Inspector General had also received thousands of complaints of potential wrongdoing related to the loan programs, and by October 2020 it had seized—with other law enforcement agencies—more than $450 million from fraudulent EIDL loans.

Two issues inherent to the emergency nature of the programs opened avenues for fraudsters: streamlined applications and a stag-

tims and posing as loan financial officers or representatives of local utilities who threaten to discontinue service if the victims do not pay immediately.

And while they were a problem before the COVID-19 pandemic, romance scams continue to evolve. Between January and September 2021, the centre received 1,291 reports of romance scams targeting 919 victims for CAD $42.2 million. These scams have become especially popular during the pandemic as more individuals moved to social media and online dating services to meet people, Labine says. Scammers typically mirror their target’s interests in their online profile, such as expressing a love for skiing on their Facebook page if the intended victim is fond the sport.



The scammer “becomes very convincing and fun to communicate with, and sometimes can be quite quick to profess their love for the victim and ask for money,” Labine says. “Other times, they establish a long-term relationship and then start asking for money. They give different reasons why they need money—there’s a family emergency, they can’t access their accounts and will pay the victims back, or they’re in the military, or there’s an inheritance and they need help to pay lawyers.”

Once fraud is reported to the CAFC, the centre can advise victims on next steps to take to protect their identities and ensure that their remaining assets are safe. The centre can also take steps on its own to disrupt fraudsters, including using its Operational Support Unit to facilitate the shutdown of a fraudulent website, disconnect numbers being used by scammers, and alert financial institutions of suspicious activity.

One major problem remains, though, for the centre to act. Less than 5 percent of victims report fraud, Labine says.

“The reason people aren’t reporting it, quite often, is because they’re embarrassed they’ve fallen victim for a scam,” Labine says. “And for seniors, they may be afraid their family will take over their account—especially if they lost a large sum of money. They don’t want the family to find out.”

Illustration by *Security Management;* iStock

gering number of loan requests. In the EIDL program, the application process was streamlined to the point that the SBA was prohibited from checking against Internal Revenue Service (IRS) tax records before granting loan approvals.

"That would be a key way for the agency to check if it was actually a business, had payroll in the last year, and met the requirements to be established," Shea says. "They would have been able to have ownership, checking against IRS records before the loans were dispersed and approved."

SBA also was dealing with the challenge of sorting through the significant number of loan applications, Shea adds, which was a tremendous push for the agency that ultimately subjected it to increased fraud.

"They issued more loans in that time period (mid-2020) than they had in the past 10 years, so they did have to make that balance," she explains. "But there were some basic things they could have done that they did not do."

For instance, SBA did not have fraud risk assessments and fraud risk profiles in place for its programs before the pandemic began.

"SBA was caught by surprise in a variety of ways, but they could have been much better prepared. They've been providing EIDL funds, and they didn't have a fraud risk assessment for that at all," Shea says. "They could have put something together. The situation is not that unusual…. We beat the dead horse of having your fraud risk assessment up front. It's going to help you figure out what levers you can pull and what you need for detection."

While it is not on the High-Risk List, the GAO has also expressed concerns about unemployment insurance and the ability to conduct oversight into how those funds were dispersed during the pandemic. Unemployment insurance is a regular program in the United States, but during the COVID-19 pandemic the U.S. federal government expanded eligibility requirements and increased the federal payouts to unemployed individuals, who typically apply online.

As of December 2021, Seto J. Bagdoyan, director, forensic audits and investigative service, GAO, says approximately $900 billion has been distributed through unemployment insurance during the pandemic. Based on prior analysis and experience, 10 percent of those funds are likely being lost to fraud.

"You're losing $90 billion off the top," Bagdoyan says. "It's probably much worse, because of the schemes that have hit the agencies and support programs."

These schemes include those introduced by organized crime efforts—originating primarily in China, Hong Kong, Nigeria, and Russia—using cyberattacks to compromise bank accounts, identities, and even mimic unemployment office websites to attract unsuspecting individuals, Bagdoyan adds. One private firm that provides cybersecurity protections to unemployment systems told the GAO that once U.S. federal funds stopped flowing into COVID-19 unemployment programs, there was a 40 percent drop in targeted attacks from organized crime entities.

"Some of these schemes will become embedded in traditional programs post-COVID," Bagdoyan says. "And then they will be revived with the next emergency on the scale that we're seeing now. It's really difficult to counter. You have to make a good faith effort to have the best set of controls you can, that you're managing as well as you can."

Some of these schemes will become embedded in traditional programs post-COVID.

The GAO has recommended that the U.S. Department of Labor create controls based on the auditor's Fraud Risk Framework, including defined and documented responsibilities and authority for managing fraud risk assessments and facilitating communication among stakeholders on fraud-related issues. As of *Security Management's* press time, the department had not agreed or disagreed with the recommendations.

Commercial-Level Fraud

Government fraud controls were not the only ones being tested during the COVID-19 pandemic. Private industries were also hit hard.

Back in April 2021, the Association of Certified Fraud Examiners (ACFE) research team had been tracking the significant level of fraud the private sector was experiencing. But it was feeling optimistic about the future. Vaccines for COVID-19 were being distributed, cases in some parts of the world were coming down, and some individuals were starting to talk about what post-pandemic life would be like.

So, in mid-2021 the team named the fourth report in its survey series on fraud and COVID-19, *The Next Normal: Preparing for a Post-Pandemic Fraud Landscape*. Since then, however, additional disruption due to large portions of the public refusing to take the COVID-19 vaccine, delays in distribution and returns to the office, and major supply chain challenges have slowed economic recovery efforts. As of 2 January, just 62 percent of eligible Americans were fully vaccinated, according to the Mayo Clinic.

"I anticipate we'll be doing a retrospect here," says Andi McNeal, CFE, CPA, research director for ACFE and one of the authors of the report, in a December 2021 interview with *Security Management*.

The findings in the fourth report, however, tracked with what ACFE has been seeing throughout the COVID-19 pandemic—fraud is up and is expected to continue to climb.

In their survey of 1,539 ACFE members in more than 100 countries, the ACFE research team found that 51 percent of respondents said their organizations have uncovered more fraud since the onset of the pandemic and 71 percent expect the level of fraud impacting their organization to continue to increase. Just 14 percent said they had uncovered less fraud.

Together, we create access for the future

Visit us at ISC West
Booth #8061

The security industry is constantly evolving in response to what is happening in the world around us. Learn how the latest developments in door opening solutions can help you provide a safer and more secure environment to address the demands of today and tomorrow.

Contact us today to discuss your specific needs and challenges:
intelligentopenings.com

ASSA ABLOY
Opening Solutions

Experience a safer
and more open world

For product info #16 securitymgmt.hotims.com

Business operations changed during the pandemic, including a shift to remote work. This adjustment opened doors for fraud.

"All controls built around in-person operations had to be reconfigured and reengineered," McNeal says. "Certain people were performing functions they hadn't before, so that's going to leave gaps as to where the security was."

For instance, many financial processes require two people to sign off on an invoice or expense before it's approved. In a physical office environment, one person could walk the invoice or expense report to the other person to sign before filing it.

Virtually, that same process can be replicated by sending the invoice electronically and having the second person sign the document using a digital signature. It's much easier, however, for a fraudster to intercept that electronic communication and insert a fake digital signature than it would be to physically intercept it or to forge it entirely.

Such an incident happened in 2020, when a director of a mobile home and residential vans company forged his estranged wife's digital signature on a loan application sent via email before liquidating the company and declaring bankruptcy. The lender went after his wife for repayment, which ultimately led to an investigation using DocuSign metadata and mobile phone location evidence to determine the husband had signed into her accounts without consent to use her signature to take out the loans.

"Companies had to shift priorities quickly and repeatedly," McNeal explains. "When the employees performing those operations are following a moving target, that can make it hard to make sure the protections we have in place are working. There's inherent friction between swift responses and controls. The faster we have to change and adapt, the more vulnerability there is."

This is especially true as 80 percent of survey respondents said cyber fraud—business email compromise, hacking, ransomware, and malware—and social engineering are the categories they expect to increase the most in the next 12 months. McNeal says an aspect of cyber fraud that is particularly challenging for organizations is the multiple motivations behind it—personal gain, political motivations, disruption intentions, or competitive reasons.

"Other risks projected to see large increases include identity crime (e.g., identity theft, synthetic identity schemes, and account takeovers), unemployment fraud, and payment fraud (e.g., credit card fraud and fraudulent mobile payments)," according to the report.

All controls built around in-person operations had to be reconfigured and reengineered.

Surprisingly, however, fewer survey respondents said they anticipated fraud growth in three areas historically used to track internal or occupational fraud: employee embezzlement (54 percent), bribery and corruption (52 percent), and financial statement fraud (47 percent).

McNeal cautions that this is still a significant portion of respondents anticipating some growth in those areas, but she says that because they are more familiar types of fraud, organizations may feel they know how to adjust their controls and processes to respond.

"We've gotten used to working remotely. We've built out our duties and are making sure they're doing that monitoring…and maybe using analytics," McNeal says. "So, in a way, those external factors are feeling harder to monitor."

Recovering the Funds

An individual fraudster might make off with a few thousand dollars, but when his or her profits are combined with others' it can create massive losses for government agencies and companies alike.

To put that into perspective, the U.S. Secret Service announced that as of 12 December 2021 it had more than 900 ongoing investigations into the fraudulent use of COVID-19 relief applications—with relief funds valued at nearly $100 billion.

"That's a combination of pandemic benefits and all the other benefits programs, too," said Assistant Special Agent in Charge Roy Dotson, who was tapped as the Secret Service's national pandemic fraud recovery coordinator, in a statement. "Every state has been hit, some harder than others. The Secret Service is hitting the ground running, trying to recover everything we can, including funds stolen from both federal and state programs."

And while individuals may be charged and ultimately convicted for fraud, it is unlikely that the money itself will be fully recovered. Arp—who previously worked in the inspector general's office at SBA and investigated EIDL fraud before joining the GAO—says it typically involves a long investigation and adjudication to forfeit those funds, whether it be a civil fraud case, criminal fraud case, restitution, asset forfeiture, or seizure of the money.

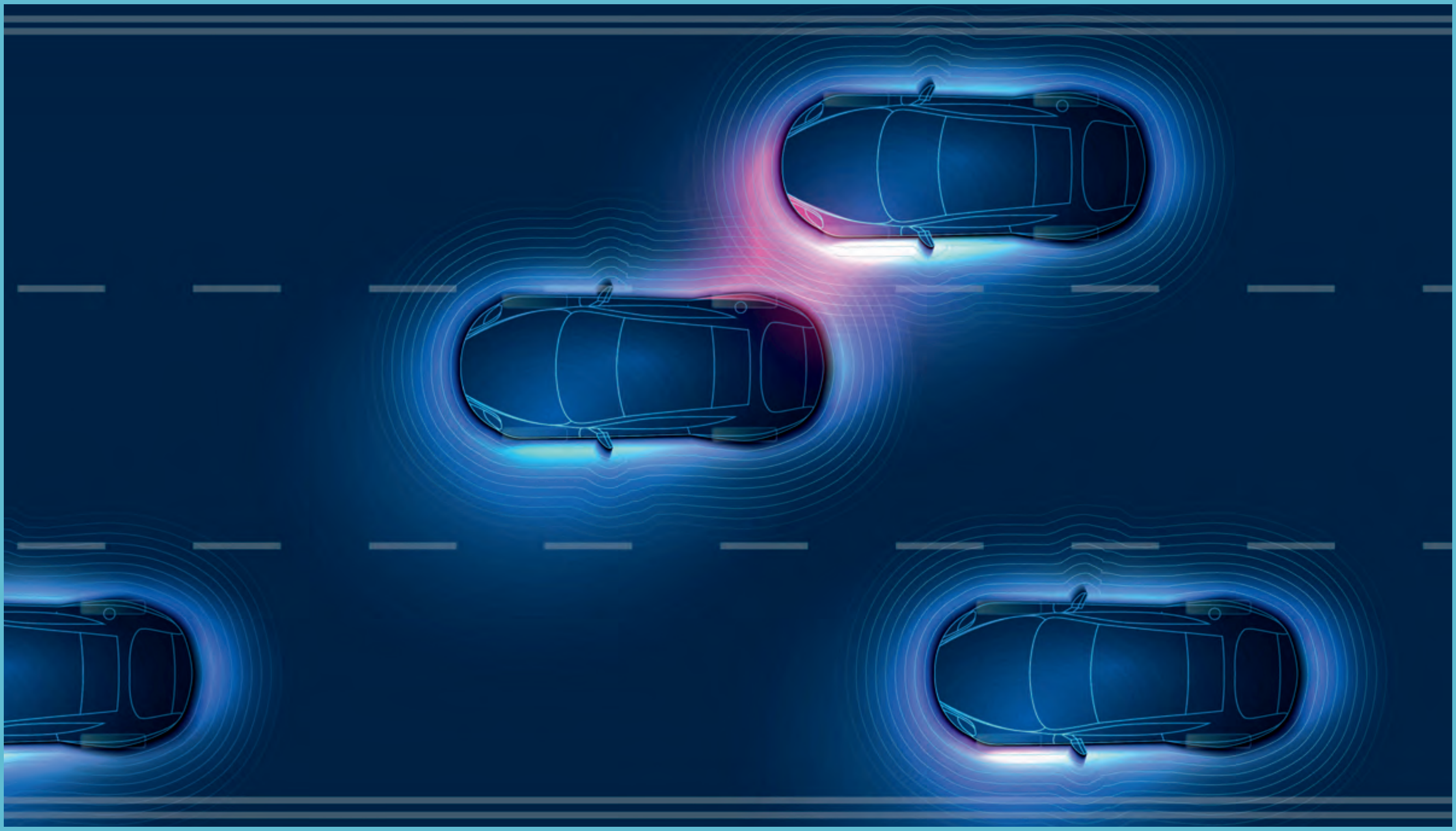
"The pandemic isn't what opened everyone's eyes," Arp adds. "They've known for years; we've made recommendations for years… and at the end of the day, it seems that there's the pay and chase model many people think is perfectly fine. But once it's gone, you might as well count it gone."

Bagdoyan agrees and says that the GAO is trying to use the national emergency of the COVID-19 pandemic as a case study for preparing agencies to have a crisis model that can be deployed on short notice to ensure there is program integrity on the front end.

"With improper payments, the recovery rate has been historically on the poor side," Bagdoyan says. "Once the money is gone, it's spent or consumed. Restitution is a very deliberate and long-term process that rarely yields full results, so you may be recovering pennies on the dollar." ■

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

SECURITY TECHNOLOGY



ON THE ROAD TO CONNECTIVITY

// By Megan Gates

The Apache Log4j Java-based logging library is used around the world to help applications, websites, and consumer and enterprise services run smoothly by logging messages to a log file or a database.

It had run largely in the background, out of sight and out of mind for most people, until 9 December 2021 when the Log4Shell zero-day vulnerability was released on GitHub. The exploit could allow an unauthenticated remote actor to take control of an affected system.

Some of those systems could include vehicles, which are becoming increasingly connected to original equipment manufacturer (OEM) back-end servers to share collected data and reliant on software to operate. Researchers investigated how Log4j was used in the automotive sector and found that electric vehicle car chargers and vehicle-to-grid (V2G) systems in Europe were at risk.

"The V2G system allows stored energy in car batteries to be redistributed over the grid to help balance demand concerning the production level," according to Upstream Security's *Global Automotive Cybersecurity Report 2022*. "In addition, they found that a car's [in-vehicle infotainment] system, which uses a complex operating system, could also be compromised. The researchers showed that by exploiting Log4j vulnerabilities, they could execute attacks on the vehicles and their connected infrastructure."

"In its *2021 Automotive Cybersecurity Report*, Upstream Security projected that connected vehicles will comprise nearly 86 percent of the global automotive market by 2025. The transformation has major ramifications for security." ■

To continue reading this article and more of the February 2022 issue, visit *asisonline.org/SecurityTechnology*

Illustration by *Security Management*

SECURITY TECHNOLOGY

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

Robotics in Security—Are They Inevitable?

PERIMETER SECURITY

By Jeffrey A. Slotnick, CPP, PSP

Due to COVID-19, other physical risks in the guarding industry, and low pay, many guarding companies are experiencing what is commonly referred to as the Great Resignation. In the United States alone, more than 38 million workers quit their jobs in 2021.

Because of the issues mentioned above, many security service providers cannot fully staff existing contracts. This makes a strong business case for robotics in the guard industry to perform repetitive tasks humans do not want to do and to enhance security functions humans must still take the lead on.

The Role of C-UAS in Perimeter Security Systems

COUNTER-UNMANNED AERIAL SYSTEMS (C-UAS)

By Kai Moncino

The military's shift to unmanned aerial systems (UAS) also accelerated the development of technologies to manufacture drones, allowing them to proliferate in commercial markets, as well. In fact, the global commercial unmanned aerial vehicle market is expected to reach $501.4 billion by 2028, registering a compound annual growth rate of 57.5 percent from 2021 to 2028, according to a new report by Grand View Research, Inc.

But for security managers at airports, nuclear power plants, oil refineries, and other critical infrastructure sites, these commercial drones pose a novel threat.

Automation Makes Security More Attainable for SMBs

COMPLIANCE

By Matt Cooper, CPP, CISSP

How can small and mid-size businesses bolster their defenses without breaking the bank? The answer can be found in the automation of security compliance.

Automation can save time and money. But it can also be a means to level the playing field for accessing the best cybersecurity for businesses of all sizes.

Automation in security compliance works well because compliance audits are largely achieved through the repetitive tasks that computers do best, such as time-intensive tasks, time-based tasks, and monitoring and reporting.

THE DROIDS YOU'RE LOOKING FOR

The COVID-19 pandemic has fast-tracked robotic adoption around the world. Sales of professional service robots increased 41 percent in 2020 to 131,800 units, according to research from the International Federation of Robotics. The *World Robotics 2021* report also found that robot density in manufacturing settings nearly doubled in 2020, reaching 126 robots per 10,000 human employees on average. South Korea, however, far outpaced the rest of the world with an average of 932 robots per 10,000 employees. The report also found that:

1 out of 3 robots built in 2020 were used to transport goods or cargo.

50+ service robot providers created disinfection robots in 2020.

End users bought **$249 million** worth of hospitality robots in 2020.

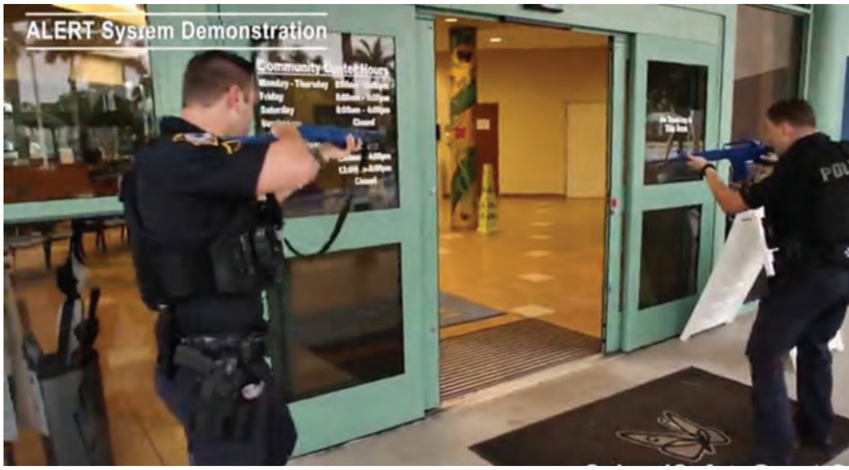
Source: *World Robotics 2021*, International Federation of Robotics, November 2021

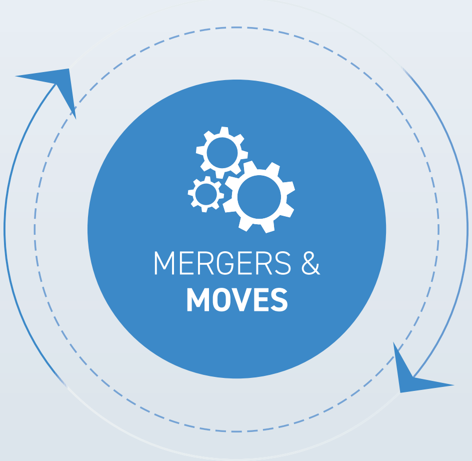
Images by iStock

ADVANCED EMERGENCY RESPONSE

The Coconut Creek Police Department in Florida provided an online demonstration of its Active Law Enforcement Response Technology (ALERT), a program that focuses on how businesses and communities at-large can be safer through immediate communication with local law enforcement. The ALERT system offers police departments real-time access to security programs and solutions, such as surveillance cameras, that are installed throughout an area and connected to the system. In an emergency, such as an active shooter situation, police officers gain direct access to live feeds from surveillance cameras, access control solutions, and public address systems.

ALERT was initially rolled out in 2020 as a way to instantly respond to attacks on schools as part of a School Safety Grant, funded by ALERT, and it has received interest from other jurisdictions, including Coral Springs, Florida, and Margate, Florida.





Allied Universal ⇆ Norred & Associates

Allied Universal acquired a full-service security firm based in Atlanta, Georgia, and New York-based MSA Security—a threat protection solutions firm.

SilverSky ⇆ Cygilant

The acquisition widens SilverSky's reach, building up its presence in the United Kingdom.

Sigma Defense LLC ⇆ SOLUTE

The acquisition of the technology and engineering firm expands Sigma's DevSecOps portfolio, gaining additional focus on cybersecurity and cloud architectures.

DigiCert, Inc. ⇆ Mocana

The purchase of Mocana will provide Internet of Things manufacturers with a fuller platform for managing device cybersecurity.

Award

The U.S. Federal Laboratory Consortium for Technology Transfer issued its 2022 Interagency Partnership Award to Liberty Defense Holdings for its millimeter-wave shoe screening technology, which can eliminate the need for passengers to remove their shoes during airport screenings.

Contract

The U.S. Department of Homeland Security's U.S. Citizenship and Immigration Services (USCIS) awarded an $81 million contract to Peraton for background investigation services.

Announcements

HelpSystems launched its Educational Partner Program, with the goal of facilitating cybersecurity learning and knowledge in college and university classrooms.

Partnerships

Testing Solutions

The Acquired Data Solutions (ADS) and Asset Security partnership will offer ADS clients additional support for automated security tools and Internet-connected devices.

Cybersecurity

Mexican broadband provider Allot Ltd. partnered with BusinessSecure to provide a zero-touch solution to protect Allot's fixed broadband small and medium-sized business and home office customers.

Active Shooter

Siemens and Shooter Detection Systems integrated their respective safe and secure building and gunshot detection technologies to improve public safety for clients.

Image courtesy of *SchoolSafetyGrant.org*

ASIS Europe 2022: A Meeting of Minds

ASIS Europe will be back in person in Prague, Czech Republic, 22–24 May 2022, for what is already shaping up to be an unmissable event for anyone needing to understand global security challenges through a European lens.

"It will be three years since our European community has been together in person, so we are quite sure there will be so much to exchange and catch up on that we won't want to spend too much time quietly listening," says Eduard Emde, CPP, ASIS Europe conference chair. "From the outset, we developed this year's program differently to maximize time for dialogue, collaborative learning, and networking."

One conference track will be dedicated to the evolving risk landscape around issues such as geopolitical tension, societal unrest, technology and the rise of AI, cyber–physical and privacy concerns, and new considerations on travel risk.

In parallel, the program will also examine how security supports business strategy, diving into what the post-UN Climate Change Conference (COP26) economy means for security teams; internal collaboration with risk management, compliance, and HR teams; how to function effectively in remote work environments; engaging the next generation of security talent; and how organizations implement enterprise security risk management (ESRM).

Plus, the innovation track will cover the latest research and developments on security tools, technology, and service solutions.

Opening with a networking function on the evening of 22 May and following with two days of conference and exhibits, the format provides an ideal opportunity to experience Prague—as well as the exceptional ASIS Europe learning on offer.

Radek Havliš, ASIS Europe conference vice-chair adds, "My hometown, Prague, is renowned as one of the world's most beautiful cities, but it is also a great business destination. The city provides a central European base for numerous global companies and is a hub for innovation and engineering. This makes an ideal combination for a long overdue gathering of our ASIS community across Europe and beyond."

The onsite event will be supplemented by two online events on 28 April and 12 May, providing maximum accessibility to ASIS's exceptional educational content.

A range of Premium All-Access passes and Free to Attend options are available for delegates, and an updated selection of sponsorship and exhibition packages offer companies a wide range of engagement, content, and brand exposure opportunities at both the online and onsite events.

Full details at *asiseurope.org*.

The State of Security Management

The ASIS Foundation's latest research—*The State of Security Management 2020, A Baseline Phenomenological and Empirical Study*—offers a snapshot of the security risk management field through the global upheaval of recent years, from pandemic and civil unrest to natural disasters and supply chain disruptions.

Through an extensive methodology, including an online survey of more than 500 professionals and interviews with 10 energetic security thought leaders, the research identifies eight key findings and four noteworthy themes about the state of security management in 2020. Key findings include:

- People matter (and by nature, security management is a "people" function, as well as a business function).
- Security executives and management professionals must embrace change.
- The security management field lacks a clear definition.
- Insularity in the security management field is a challenge.
- ESRM is catching on and is considered viable.
- Security professionals need to broaden their perspectives on global threats.
- The security profession's brand and reputation must be enhanced.
- Security management metrics are an increasingly essential tool.

The report concludes with 14 recommendations meant to be actionable steps, addressed to a variety of audiences including security professionals, employers, academics/researchers, C-suite executives, and related professional associations.

ASIS members can access the full report for free. Learn more about the report and help fund future research by donating to the ASIS Foundation at *asisfoundation.org*.

Foundation Scholarships

Apply now for one of 30 ASIS Foundation Certification Scholarships. Deadline: 15 April 2022. Learn more at *asisonline.org/foundationscholarships*.

Member Appreciation Month

To thank you for your loyalty, ASIS is celebrating members all March long—offering access to great prizes, member-exclusive content, and special savings on ASIS professional development resources. Visit the Member Appreciation Month homepage at *asisonline.org/MAM* each week in March to discover featured content, discussions, and deals.

ASIS Global Events

MAY

22-24 ASIS Europe – Prague, Czech Republic

ASIS Education Webinars

MARCH

8 How Strong is Your ESRM Game? ESRM Maturity Model

22 Traversing the Corporate Ladder: Skills and Attributes for the Next Generation of Senior Business Leaders

APRIL

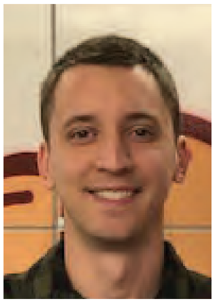
5 How Does Crisis Management Response Become Your Business Continuity Plan?

12 ESRM Decision-Making for Stakeholders

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

Young Professionals Corner

Security Management gets the perspective of Young Professional Community liaisons from ASIS International's Buenos Aires, Argentina, and Jamaica chapters.



Pablo Nicolas Espinosa, APP, PSP

Seasoned professionals might be inclined to address contemporary security challenges with the same time-tested mind-set and toolbox that may not be the most suitable approach to these more complex times. This gives young security professionals a chance to fill in the gap by offering newer perspectives that could result in a more fitting solution, thus hardening the organization's resiliency.

Javan Simpson, PCI

The world is changing. People everywhere are gaining higher appreciation for the importance of security, and the demand for professionals in all areas is growing. ASIS has given me the opportunity to interact with and learn from some of the brightest minds in the global security community, hone my skills, and improve my competence level.

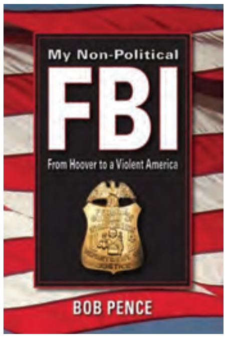
Member Book Review

My Non-Political FBI: From Hoover to a Violent America. By Bob Pence. Fulcrum Group; fulcrumgroupbooks.com; 336 pages; $30.

My Non-Political FBI is a meticulously researched and carefully written autobiography by former FBI Special Agent in Charge (SAC) Bob Pence.

Pence describes his early days growing up watching newsreels of WWII bombings, hearing air-raid sirens, and being visited by block wardens. This instilled in him a respect for safety and security. As an adult, he enlisted and served as an officer in the U.S. Army.

During this time, he weighed a career as a military officer or FBI agent. In either capacity, he knew he would devote his life to serving public safety.


My Non-Political FBI

From Hoover to a Violent America

BOB PENCE

Within weeks of finishing up his tour, he received a letter of appointment from FBI Director J. Edgar Hoover and embarked on a rewarding 30-year FBI career.

Pence began his FBI career in Mississippi during the 1960s, investigating civil rights violations. He rose through the ranks before finally retiring as SAC of the Denver Field Office. His career touched on investigations of approximately 200 violations under FBI purview. In this book, Pence provides an insider's view of a wide range of cases that he either investigated or supervised.

My Non-Political FBI is a primer for FBI personnel and security professionals who want to understand how the Bureau's methods and mission have evolved from the 1960s to present day. Pence writes in a style that is self-effacing and at times mixed with touches of humor, but never wavering in his commitment to public service, safety, and adherence to the U.S. Constitution.

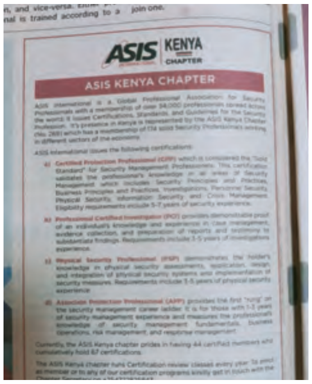
Following his retirement, Pence has engaged in public speaking, volunteered to develop best practices for assisting troubled youth, and consulted in public and corporate security across the globe.

Reviewer: R. Scott Decker, PhD, is a retired FBI special agent with experience in violent crime, terrorism, and physical security. His book, Recounting the Anthrax Attacks: Terror, the Amerithrax Task Force, and the Evolution of Forensics in the FBI, *has won awards for nonfiction, true crime, and science and technology.* ■

#MYASIS IMAGE OF THE MONTH

ASIS WIS KENYA CHAPTER

In the *Business Daily Today,* page 6... A Feature of the ASIS Kenya Chapter... Did you know that currently, the ASIS Kenya chapter prides in having 44 certified members who cumulatively hold 67 certifications. The ASIS Kenya chapter runs Certification review classes every year. #MyASIS


...n, and vice-versa. Either ... join one.
...nal is trained according to a

ASIS | KENYA CHAPTER

ASIS KENYA CHAPTER

ASIS International is a Global Professional Association for Security Professionals with a membership of over 34,000 professionals spread across the world. It issues Certifications, Standards, and Guidelines for the Security Profession. It's presence in Kenya is represented by the ASIS Kenya Chapter (No. 269) which has a membership of 174 solid Security Professionals working in different sectors of the economy.

ASIS International issues the following certifications:

a) Certified Protection Professional (CPP) which is considered the "Gold Standard" for Security Management Professionals. This certification validates the professional's knowledge in all areas of Security Management which includes Security Principles and Practices, Business Principles and Practices, Investigations, Personnel Security, Physical Security, Information Security and Crisis Management. Eligibility requirements include 5-7 years of security experience.

b) Professional Certified Investigator (PCI) provides demonstrable proof of an individual's knowledge and experience in case management, evidence collection, and preparation of reports and testimony to substantiate findings. Requirements include 3-5 years of investigations experience.

c) Physical Security Professional (PSP) demonstrates the holder's knowledge in physical security assessments, application, design and integration of physical security systems and implementation of security measures. Requirements include 3-5 years of physical security experience.

d) Associate Protection Professional (APP) provides the first "rung" on the security management career ladder. It is for those with 1-3 years of security management experience and measures the professional's knowledge of security management fundamentals, business operations, risk management, and response management.

Currently, the ASIS Kenya chapter prides in having 44 certified members who cumulatively hold 67 certifications.

The ASIS Kenya chapter runs Certification review classes every year. To enrol as member or to any of our certification programs kindly get in touch with the Chapter Secretary on [illegible]

ASIS CERTIFICATION PROFILE // VASHITA MEHRA, CPP, PCI, PSP

> *"When you study so much on a subject, it seeps into your thought-process and behavior. Because of these certifications, I was able to fine-tune my internal security processes and enhance my security procedures."*

When Vashita Mehra was transitioning out of military service in 2008, she knew that her corporate future would involve security management.

"This is where my passion and expertise lie," she explains. "The constant evolution of this field in terms of technology, new concepts, and new challenges excites me."

In building her career, Mehra says she wanted to demonstrate that the notion that security is a "man's domain" is a myth. "I just could not understand what was so man-specific about security management that a woman could not do it. I wanted to get in here and make a place for myself and others, too," she says.

She oversees security operations for India for an international multibillion-dollar risk management firm. Also, she's one of 28 women worldwide—and the only woman in India—who hold the ASIS board certification triple crown.

"I started my certification journey with the aim of attaining the Certified Protection Professional (CPP®) designation," she shares. "I wanted to do this because it is one of the most difficult security certifications, and I wanted to understand the concepts therein."

She passed the exam on her first attempt—and was hungry for more. She studied for the Professional Certified Investigator (PCI®) exam—"an extremely interesting subject" she studied "more out of interest with the subject than with the aim of passing the exam"—and passed that as well. Wanting to complete the set, she studied for and passed the Physical Security Professional (PSP®) exam soon after.

"The amount of knowledge required for these certifications is immense," she says. "When you study so much on a subject, it seeps into your thought-process and behavior. Because of these certifications, I was able to fine-tune my internal security processes and enhance my security procedures."

Given the boost that she experienced in her professional security practice and the accolades and recognition that she has received from her peers since attaining the ASIS certifications, Mehra's response to those considering whether to similarly pursue certification is simply: "Go for it."

Profile by **Steven Barnett,** ASIS communications specialist

ACCELERATE YOUR SECURITY CAREER WITH ASIS CERTIFICATION

CPP® PCI™ PSP™ APP

ASIS certification has the potential to boost your annual salary and your career prospects—just like it's done for thousands of successful ASIS-certified professionals.

20%
more

ASIS-certified professionals earn 20% more than their non-certified colleagues

54%

of ASIS certificants received promotions or an increased salary by becoming certified

55%

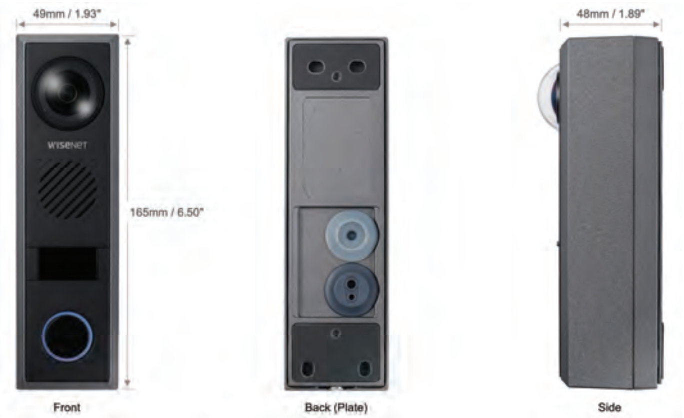
of security industry employers require or prefer to hire ASIS-certified candidates

According to ASIS International's 2019 certification survey

ASIS INTERNATIONAL

Get started today.
asisonline.org/certification

PRODUCT SHOWCASE



TOUCHLESS INTERCOM SYSTEMS

Hanwha Techwin's TID-600R Network Intercom Station offers a touchless call system where users can simply present their palm within six inches of the station to initiate a call. The unit features a 2MP sensor with Hanwha Techwin's signature WDR and IR. The station also features echo cancellation, noise reduction, and a built-in tamper switch and relay for standalone door access. Users can create audio messages to be played when the device is approached or upon call initiation. It can also integrate with various VMS, access control, SIP phones, or PBX servers. Visit *hanwhasecurity.com/product/tid-600r* to learn more. **Stand 14079, Circle 101**

ACCESS CONTROL

AirAccess from **NAPCO** is a cell- and cloud-based hosted access system, powered by StarLink cellular communications. No server or on-site security staff is needed; instead, the system is scalable and easy to add on to doors with wireless smart locks that retrofit any standard locks or use standard identification readers with wireless panels. AirAccess also offers an app with built-in mobile credentials, text alerts, and lockdown—all for a flat monthly rate per system. Visit *airaccesscontrol.com* to learn more. **Stand 12031, Circle 102**

AirAccess
Access Control Made Easy
• Easy to Afford Monthly Flat Rate per System
• Mobile App & Credentials w/ SMS Texts & Lockdown
• Right-Sized for Small & Medium Businesses
NAPCO Access
ISC West Booth 12031

TAILGATE PREVENTION

Detex offers panic hardware for restricted secure areas and internal departments, including building entrances, manufacturing facilities, office entrances, fitness centers, corporate offices, and record rooms. The hardware aims to deny unauthorized entry while smoothly facilitating authorized entry. The Tailgate Detection System offers operations a chance to limit access to one identified entrant without giving tailgaters a free pass. The solution is compatible with most access control technologies, can be retrofitted, and features an integrated door prop alarm for additional security. Visit *detex.com* to learn more. **Stand 13114, Circle 103**

KEY MANAGEMENT

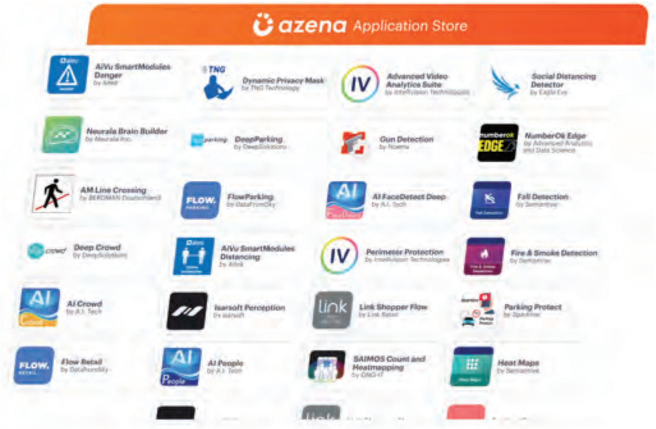
Morse Watchmans, Inc., offers signature key management systems that have customizable modules to secure all facility keys and assets, including wallets, cell phones, laptops, and small weapons. The company is dedicated to helping businesses maintain a secure and safe environment, and it looks forward to developing more progressive business security products in the future. Visit *morsewatchmans.com* to learn more. **Stand 15109, Circle 104**

LOGISTICS SOFTWARE

Technology from **TEAM Software** by WorkWave offers security contractors increased efficiency and a chance to streamline operations. This holistic software gives users a way to keep an eye on all the moving parts of a business—insight into employee engagement, customer satisfaction, and overall efficiency allows for data driven decisions. Visit *www.teamsoftware.com/industries/security-guard-software* to learn more. **Circle 105**

CABINET LOCKS

ASSA ABLOY's new HES KS210 integrated access control server cabinet lock offers enhanced security communications, monitoring, and credential options with integrated RS-485 OSDP and BLE technology. These locks provide a way to protect mission-critical data and equipment across an organization. Visit *hesinnovations.com* to learn more. **Stand 8061, Circle 106**

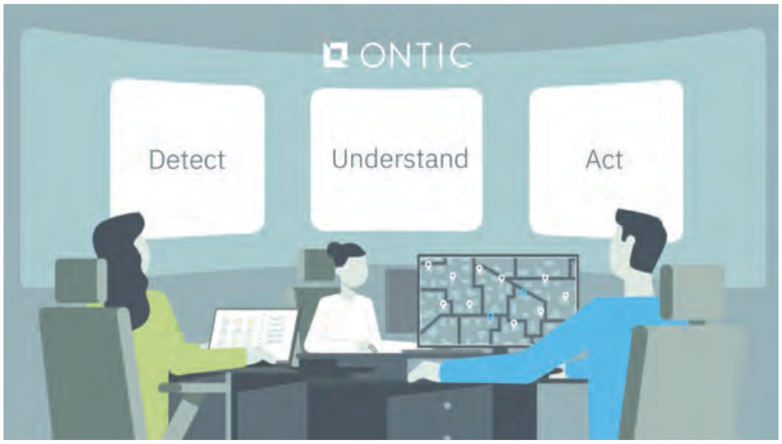


VIDEO ANALYTICS

Azena's platform for smart cameras offers ready-to-use artificial intelligence-enhanced video analytic applications, which can run directly on a smart camera to provide flexible video analytics solutions for unique business needs. More than 100 apps are available in the Azena applications store for smart cameras, offering solutions for retail, manufacturing, logistics, parking, stadiums, and more. The Azena camera operating system allows cameras to simultaneously run several apps downloaded to the cameras and changed based on customer needs. Visit *azena.com* to learn more. **Stand 23075, Circle 107**

MAIL SCREENING

RaySecur's MailSecur solution offers the first U.S. Department of Homeland Security Safety Act-designated millimeter wave (mmWave) desktop scanner that can see into mail and packages to detect threats, including liquids, powder, explosives, weapons, radioactive materials, and other suspicious contents. The solution features a resolution 10 times greater than airport scanners and 300 times more sensitive than x-rays when it comes to detecting liquids and powder. MailSecur includes the turnkey EODSecur mail security program, which includes training, development of standard operating procedures and response plans, and one-touch, around-the-clock access to trained military Explosive Ordnance Disposal professionals who can immediately assist users working to resolve a threat. Visit *raysecur.com/mailsecur* to learn more. **Stand 21125, Circle 108**



THREAT DETECTION

Ontic's real-time threat detection offering connects the entire threat management landscape and investigation process for Fortune 500 and emerging organizations, offering a picture of the risks that an entity faces. Key features include high-impact weather alerts and categorization connected to workflows that can activate a coordinated response; interactive and layered visualization of critical signals from OSINT, social media, the Dark Web, and news sources; continuous gathering of real-time and historical data; and customizable alert configurations for active events and known risks to assess threat relevance related to important people and places. Visit *www.ontic.co* to learn more. **Stand 5059, Circle 109**

EXTERNAL POWER SUPPLY

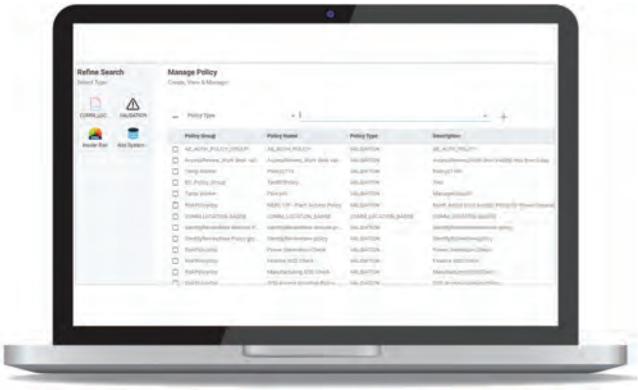
Beginning in Q2 2022, **ComNet** will introduce two hardened PoE power injectors for applications where higher requirements for PoE power. The CNGE1IPSBT hardened Ethernet PoE power injectors meet the IEEE802.3bt standard and can supply power to devices requiring more power than provided by IEEE 802.3 at/af. The unit is AC-powered and the CNGE1IPSBT/DC model is DC-powered. Both models feature auto-detection of powered devices and are ideally suited to fiberoptic, wireless, or other networks where there may be difficulty in furnishing operating power to the powered devices. Visit *www.comnet.net* to learn more. **Stand 30070, Circle 110**

GUARDHOUSES

Par-Kut offers an enhanced bullet-resistant security booth, developed in collaboration with the integrator and end user. Featuring ballistically protected walls, glass, and doors, these guardhouses are designed to complement the architecture of the facilities they serve. Factory-assembled Par-Kut security booths have exterior trim below the window line, as well as a decorative parapet around the top that conceals the rooftop air conditioning unit from pedestrian sightlines. Like all Par-Kut buildings, the bullet-resistant booths also include factory-installed electrical systems and are pre-finished in the customer's choice of color. Visit *www.parkut.com* to learn more. **Circle 111**

TURNSTILES

Designed Security Inc.'s ES9000 is designed for building lobby applications that call for higher security and high speed throughput while maintaining interior aesthetics. This unit—an IP-based optical turnstile with swing gates—offers a visual and psychological barrier, so incoming pedestrians know authorization is required to enter secured areas. The turnstile can monitor high throughput traffic flow of up to 60 people per minute per lane, and optical sensors and gates make sure that each authorized credential only allows for a single person to enter. The unit can also be customized to meet various security and architectural requirements. Visit *dsigo.com/products/optical-turnstiles/ES9000* to learn more. **Stand 13114, Circle 112**



ACCESS CONTROL

With policy-based access control (PBAC) from **Alert Enterprise,** users can adjust to today's increasing shift to hybrid work environments, adapting to sporadic schedules and overcoming legacy physical access control system limitations and manual requirements. Instead of assigning perpetual access privileges to each cardholder, PBAC offers a cloud dynamic authorization service for physical access. Using identity, roles, and policies, PBAC determines access rights to buildings and physical spaces in real-time without the need to fully replace existing access components. Visit *alertenterprise.com* to learn more. **Stand 6071, Circle 113**

REMOTE POWER SUPPLY

Altronix will be showcasing its NetWaySP4BTWP hardened 802.3bt PoE switch, which provides up to 90W per port for a total of 240W. This unit can deploy high-powered devices, including IP cameras, illuminators, wireless access points, and more. It also features four PoE ports and dual SFP ports, which support single/multi-mode fiber, and includes a built-in battery charger for a LiFePO4 battery. Visit *www.altronix.com/products/NetWaySP4BTWP* to learn more. **Stand 11073, Circle 114**

PERIMETER PROTECTION

Together with **Axis** cameras, the Perimeter Defender is an artificial intelligence-based solution that offers analytics gathering intel from the edges of a facility. This solution provides automatic detection and classifies and responds to people and vehicles intruding on a property—giving users the chance to quickly and appropriately respond. The AI-based functionality allows for an easy setup without the need for manual calibration. When used in conjunction with Axis pan-tilt-zoom cameras, thermal cameras, and audio speakers, it offers a system applicable for high-security locations. Visit *axis.com/products/axis-perimeter-defender* to learn more. **Stand 14051, Circle 115**

SECURITY OPERATIONS CENTER GOVERNANCE

Vector Flow, Inc's security operations center (SOC) governance application offers security managers a chance to measure, control, and direct SOC operations on a global scale and make proactive decisions. With the SOC governance application, security managers can continuously monitor and assess an organization's current state, including SLA measurement of alarms, identifying and detecting false and nuisance alarms, and analyzing the performance and outcomes for each SOC technician and SOC itself. Visit *www.vectorflow.com* to learn more. **Circle 116**

INTELLIGENCE ANALYSIS

Resolver's risk intelligence platform offers security leaders additional visibility and insights for the chance to allocate resources and make the greatest impact. With applications for incident management, case investigations, security operations, and risk, Resolver offers a wide range of solutions and currently works with more than 1,000 leading organizations. Visit *resolver.com* to learn more. **Circle 117**

Judicial Decisions

Negligence. Patrol security services company Asset Overwatch Services will pay $2 million to settle a lawsuit in response to the 2019 death of a Florida man who was killed inside his apartment at a complex Asset was contracted to protect.

Asset was the contract security provider for the building Kemoze Chambers lived in, which was managed by Silver Oaks Property Holdings and Blue Magma Residential. On 23 August 2019, someone shot and killed Chambers inside his apartment. The gunman remains at large.

Chambers' mother sued Asset, Silver Oaks, and Blue Magma on behalf of her son's estate. She claimed Asset had an insufficient number of competent security guards in visible areas to deter criminal activity. She also alleged that the property lacked adequate security measures, despite receiving notices about its insufficiencies.

The suit also alleged that all three defendants failed to take necessary precautions to protect residents from "reasonably foreseeable criminal acts," especially given the building's location in a high crime area, with assaults, shootings, robberies, and other crimes occurring on or near the building's premises. (*Wright v. Silver Oaks Property Holdings LLC et al.*, Orange County Circuit Court, No. 2021-CA-003426-O, 2021)

Money laundering. A U.S. federal judge sentenced former U.S. Drug Enforcement Agency (DEA) officer Jose Irizarry to serve more than 12 years in prison for conspiring with a Colombian drug cartel to launder money.

Irizarry—who pled guilty in September 2020 to 19 charges, including bank fraud and aggravated identity theft—became involved in the scheme soon after he filed for personal bankruptcy protection in 2010.

According to court documents, Irizarry leveraged his standing as a special agent for the DEA to reroute an estimated $9 million from undercover money laundering investigations to himself and other conspirators. He used a stolen identity to open a bank account that received the diverted funds. Irizarry received at least $1 million in bribes and kickbacks.

Along with the 145-month prison sentence, Irizarry was ordered to pay $11,233 in restitution and relinquish his interests in items, including a luxury sports car.

During court proceedings, Irizarry insisted that the DEA had a culture of corruption, and U.S. District Court Judge Charlene Honeywell noted a need for additional investigations into potential corruption of other agents. (*United States v. Jose Irizarry,* U.S. District Court for Southern District of New York, No. 19-cr-913, 2021)

Irizarry's wife, Nathalia Gomez-Irizarry, was also charged with involvement in the conspiracy. Gomez-Irizarry entered into a plea agreement with the government—she pled guilty to one count of a conspiracy to commit money laundering and was sentenced to five years of probation, during which time she must perform 50 hours of community service. She was also ordered to pay a fine and forfeit a Tiffany diamond ring. (*United States v. Nathalia Gomez-Irizarry,* U.S. District Court for Middle District of Florida, No. 20-cr-00077-CEH-TGW, 2020)

Legislation

Austria

Mandatory vaccinations. Austria enacted legislation that requires COVID-19 vaccinations for all residents through at least January 2024.

With the COVID-19 Compulsory Vaccination Act (164/ME XXVII.GP), the country became the first Western democratic nation to make these vaccinations mandatory. Exemptions are only available for pregnant women and people who cannot receive a vaccine for medical reasons or who recovered from a coronavirus infection in

LEGAL HIGHLIGHTS

COURT CASES

Issue: Espionage
Case: *United States v. Lieber*
Venue: U.S. District Court for Massachusetts
Status: Convicted
Significance: Lieber was found guilty of lying about his involvement with China's Thousand Talents Program.

Issue: Retaliation
Case: *EEOC v. Hyde Bellagio*
Venue: U.S. District Court for Nevada
Status: Settled
Significance: A former Las Vegas nightclub will pay $1 million to settle sexual harassment and retaliation charges.

Illustration by iStock, *Security Management* the past six months. The Austrian government is enforcing the federal law with financial penalties for those who refuse to get vaccinated. People 18 years or older who are not vaccinated may be fined up to €3,600 ($4,000) every three months.

At the end of 2021, Austria had one of the lowest vaccination rates in Western Europe, with less than 70 percent of its population identifying as fully vaccinated.

United States

Artificial intelligence. U.S. senators passed a bill that would create a new training program for corporate staff that acquire and manage artificial intelligence (AI) technology.

As part of the Artificial Intelligence Training for the Acquisition Workforce Act (S. 2551), the U.S. Office of Management and Budget would be responsible for providing the training, plus regularly updating the program.

The bill was sent to the U.S. House of Representatives for consideration.

Regulatory Decisions

Norway

Privacy. The Norwegian Data Protection Authority (NDPA) fined LGBTQ+ dating app Grindr a record 65 million Norwegian kroner ($7.2 million) for violating the EU's General Data Protection Regulation (GDPR).

The NDPA determined that Grindr breached user consent requirements when it divulged users' personal information to third parties for marketing; the third parties were also able to share that data with others. The information could be used to identify users and included GPS locations, IP addresses, age, and gender.

The NDPA determined that the data from Grindr could place users at physical risk.

"…Grindr users in Norway may have ties to territories where sexual minorities face persecution," according to the NDPA's decision. "…Risks may also apply if the individual belongs to certain conservative religious communities in Norway or abroad."

The NDPA's decision also disagreed with Grindr's argument that physical and digital worlds are segregated and the disclosure of users' personal information is unlikely to result in prejudice or discrimination in the real world.

Grindr notified users about how their data would be shared, but the notice was part of the privacy statement that users were forced to accept to use the app. Using this process meant Grindr did not obtain consent to share user data, the NDPA said, especially given that information about the disclosure of personal data was either mostly unclear or inaccessible to users.

The authority began investigating this issue in January 2020 at the request of the Norwegian Consumer Council.

This fine is the highest the authority has levied against an entity. The NDPA originally intended to fine the dating app 100 million kroner ($11 million), but the fine was decreased after Grindr provided information about its financial situation.

"In this case, we imposed a high violation fee, because we believe the violations are very serious," Bjørn Erik Thon, director of the NDPA, said in a press release. "Thousands of users in Norway have had their personal information illegally disclosed for Grindr's commercial interests."

United States

Unfair advantage. The U.S. Government Accountability Office (GAO) determined that in putting together an ultimately successful bid to secure a $400 million U.S. Navy contract, Booz Allen Hamilton had an unfair advantage.

Booz Allen's use of insights from two retired Navy captains gave it an unfair competitive edge with information that was not publicly available, according to the December 2021 audit.

The GAO gave the Navy two options to mitigate the issue. It must either disqualify Booz Allen from consideration for the contract, or it must "neutralize" the impact of the information that the former Navy captains had and consider revised bids. ■

International Legislation

Hong Kong

Censorship. Hong Kong recently amended its National Security Law, allowing the government to censor movies.

The Film Censorship Bill 2021—approved by Hong Kong's legislative council—allows for certain films to be banned if they violate the National Security Law. Violations can include encouraging, glamorizing, promoting, or otherwise supporting prohibited acts such as secession, cooperating with foreign governments or entities, engaging in subversion, or terrorism.

Anyone who screens banned films could face monetary fines as high as HK$1 million ($130,000), as well as a three-year prison sentence. Authorities do not require a warrant to search venues that screen movies, including theaters and company offices. The amendment does not apply to movies distributed online.

The amendment allows the chief secretary of Hong Kong to retroactively ban movies that were released with approval. The authority may also demand additional information about screenings.

Although proponents of the bill said the censorship will support national security, critics of the new legislation said it will likely suppress cinematic creativity.

Hong Kong's National Security Law was enacted in June 2020 after a series of pro-democracy protests. The security law vaguely established that actions, speech, or other forms of support could be a criminal offense if considered collusion with a foreign entity, secession, subversion, or terrorism.

Issue: Spyware
Case: *Apple Inc. v. NSO Group, et al.*
Venue: U.S. Dist. Ct. for N. Dist. of California
Status: Filed
Significance: Apple alleges that the spyware maker and its parent company illegally surveilled Apple users.

LEGISLATION

Issue: COVID-19
Bill: No. 327
Venue: National Assembly of France
Status: Enacted
Significance: Requires people to be fully vaccinated against COVID-19 to participate in activities.

Issue: Defense
Bill: H.R. 4350
Venue: U.S. House of Representatives
Status: Passed
Significance: Addresses Havana Syndrome and military sexual assault, but does not establish a Cyber Incident Review Office.

MARKETPLACE

Included in this month's solutions are license plate readers, video management solutions, access control systems, and more.

#301

License Plate Readers

Genetec announced the next generation of its AutoVu SharpV automatic license plate recognition (ALPR) camera. The latest version offers a fixed ALPR solution that can be used anywhere. Along with machine learning and analytics, it can also perform in all conditions. The camera can be installed and running within minutes due to features including embedded 4G/LTE/GPS, plus motorized lenses with zoom and auto-focus. It can monitor entrances and exits, capture license plates on city streets and highways, manage off-street parking lots, and cover access points to search for wanted vehicles. Built-in illuminators, shutter, and high-resolution sensors offer users sharp images for any time of day or night, while vehicle analytics can provide information on vehicle type, color, and the speed and direction it was traveling.

www.genetec.com

#303

Video Management

Johnson Controls announced a recording solution, VideoEdge 2U High Capacity Network Video Recorder (NVR), which combines the capabilities of victor with the intelligence from VideoEdge NVRs. Fueled by Tyco Artificial Intelligence, the solution offers actionable insights and allows users to manage dozens of cameras at full frame and resolution rates. Users can record in RAID configurations up to 100 terabytes. They can take advantage of 12 front-accessible storage drives, which can be hot swapped while recording. This solution offers a redundant power supply and the ability to deploy cameras with an open architecture, adding and reassigning licenses at any time.

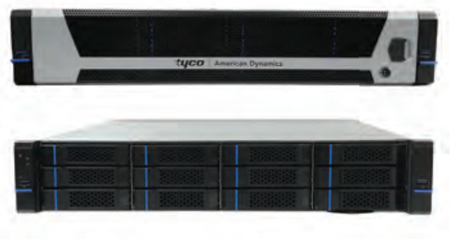
www.americandynamics.net

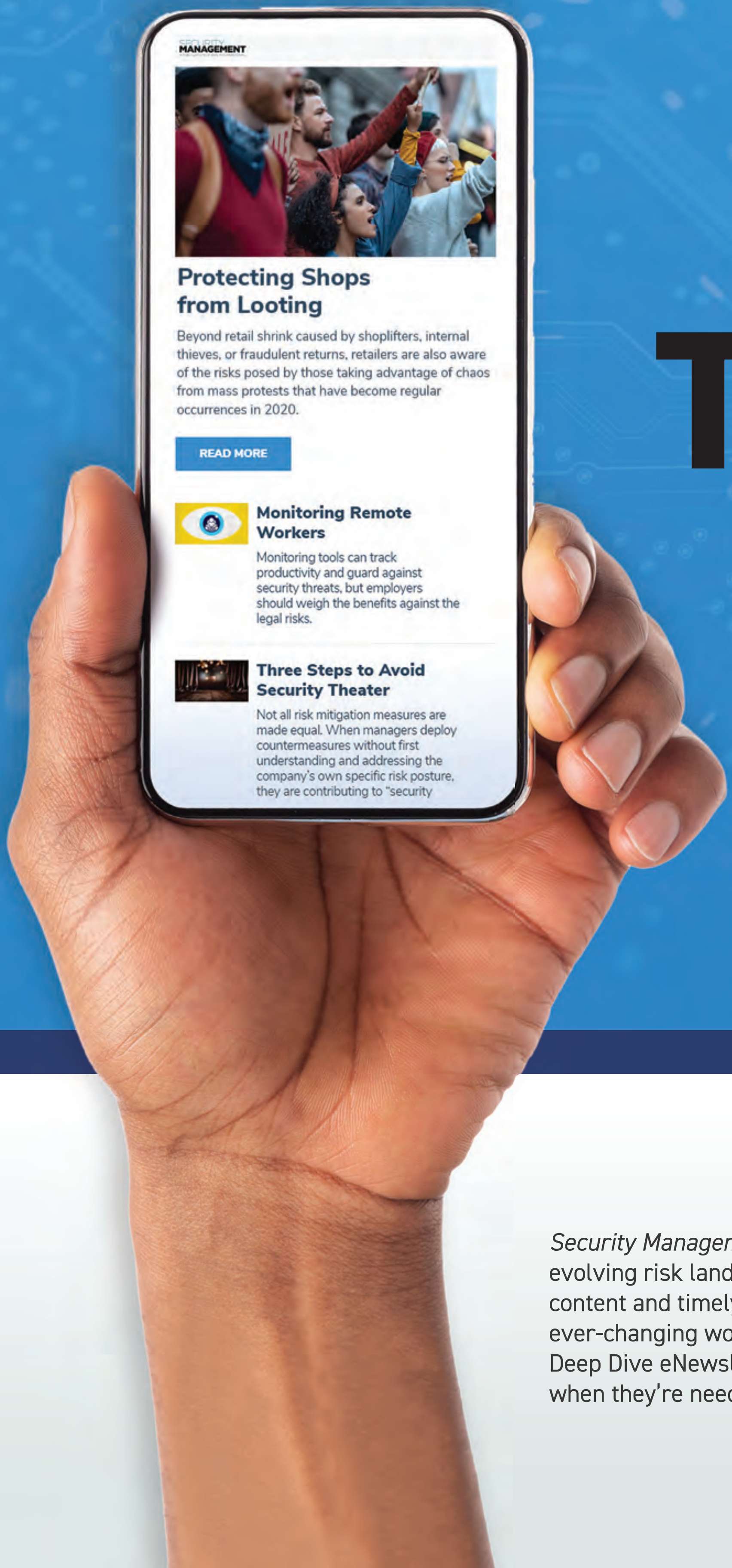
#302

Moving Surveillance Camera

Bosch introduced its Autodome IP starlight 5100i IR moving camera with a 1.1/8-inch sensor, offering 4-megapixel resolution and 30x optical zoom. It also offers HDR X combined with starlight technology and dual illumination—integrated IR and white light—which captures images that can distinguish between individuals and objects. The camera's built-in artificial intelligence supports operators with object detection in areas of interest, even while idle, allowing for increased safety in city and perimeter environments. Capable of withstanding the elements, it includes an automatic rain-sensing wiper to keep images clear, and it is weatherized with an IP66 rating and vandal-resistant with IK10 housing.

www.boschsecurity.com





#304
Cloud Video Storage

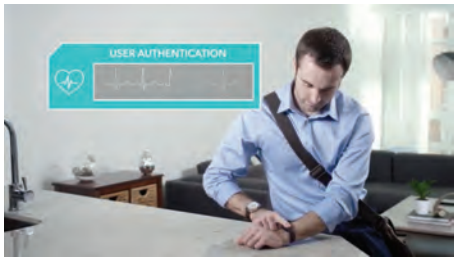
Videoloft's cloud video surveillance platform offers a remote recording solution for users and provides resellers with a potential revenue stream when added to offering portfolios. For large surveillance system clients, the solution delivers secure offsite video backup, while small and medium-sized businesses can record up to 8MP direct to the cloud—allowing for a remote standalone storage solution. The platform provides system integrators and resellers with video software as a solution (VSaaS) for any size system or vertical application.
www.videoloft.com

#305
Access Control

ProdataKey (PDK) introduced four new controllers, expanding its high-security Red series. The PDK Red 8 and Red Max are all-in-one multi-controller and power supply enclosures for ordering and installing access control components for mid- to large-scale commercial projects. They feature a 10-amp power supply and streamline installation by reducing the complexity of cables for access control networks. The Red Gate and Red Pedestal, available with either Wimac wireless or Ethernet connectivity, offer security to a range of outdoor areas, including athletic fields, garages, gated entrances, loading docks, and parking lots.
www.prodatakey.com

#306
Biometrics

Nymi and Giesecke+Devrient (G+D) developed a biometric wristband solution that offers companies and their employees a different approach to securely access a workplace. The wearable solution allows an employee passwordless and handsfree access, with users following a Privacy by Design and zero-trust security framework. The wristband is activated by fingerprint and heartbeat, authenticated by a mathematical template stored in the wristband's internal chip. The Nymi Connected Worker Platform ensures interoperability with other security components across digital systems, physical environments, and corresponding networks.
www.nymi.com



#307
Air Quality

Senstar announced an integration of its Symphony Common Operating Platform with the HALO IoT Smart Sensor from IPVideo Corporation. The integration expands services for HALO users, including the ability to monitor alerts and notify staff about abnormal ranges of sounds, such as a gunshot; chemicals; and air quality and health, such as vaping. HALO helps provide immediate alerts to a facility's occupants about dangerous conditions caused by airborne diseases or other threats, even in areas where video surveillance would be inappropriate, such as restrooms, locker rooms, hotel rooms, and hospital patients' rooms.
www.senstar.com

ADVERTISERS INDEX

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

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

advertisers online

Altronix
www.altronix.com

Ameristar
www.ameristarfence.com

Assa Abloy
www.intelligentopenings.com

Axis Communications
www.axis.com

Comnet
www.comnet.net

Detex Corportation
www.detex.com

Hanwha Techwin
www.hanwhasecurity.com

Metro One Loss Prevention Group
www.metroonelpsg.com

Par-Kut International
www.parkut.com

Prosegur
www.prosegur.us

Rologard
www.rologard.com

Speco Technologies
www.specotech.com

Special Response Corporation
www.specialresponse.com

Starlink/Napco
www.starlinkfire.com

Vector Solutions
www.vectorsolutions.com

Zbeta Consulting
www.zbeta.com

Do You Feel Safe?

While the COVID-19 pandemic shook up business routines, supply chains, and health, it did not fundamentally alter how safe people feel worldwide. According to the Gallup *2021 Global Law and Order Index*, the level at which people across 115 countries were confident in their local police, felt safe in their communities, or were victims of theft or assault in 2020 remained relatively steady, although there is always room for improvement.

Global Score

82 out of 100

Regionally, scores changed little in 2020, although declines in sub-Saharan Africa—especially Cameroon, Guinea, Kenya, Mali, and Nigeria—contributed to a two-point drop in the region's score. In particular, Nigerians' confidence in local police dropped from 55 percent in 2019 to 40 percent in 2020 following violent protests against alleged police brutality.

Top Scoring Countries

94	Norway
93	United Arab Emirates
93	China
93	Switzerland

Lowest Scoring Countries

57	Uganda
57	Guinea
53	Gabon
53	Venezuala

What Makes a Country Feel Safe?

Gallup measured safety based on four key elements, which have largely remained unchanged globally since 2017, according to *Gallup World Poll* findings. Ratings were based on a poll of more than 120,000 adults in 115 countries in 2020.

72%

said they feel safe walking alone at night where they live.

71%

have confidence in the local police.

13%

had money or property stolen from them or another household member in the past year.

6%

said they were assaulted or mugged in the past year.

Infographic design & illustration by Mariah Bartz, iStock

Don't Wait Until It's Too Late

Save Time, Lives & Money. Replace POTS lines on Fire Alarms Today with Leading Fire Cellular for All FACP Brands

Compliances (Radio): NFPA 72 2019, UL 864 10th Ed, CSFM, LAFD, NYC FD

- **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 Cellular Communicators***
- **Supports Any 12V/24V Fire Alarm Panel, new or old – StarLink Panel-Powered Cell Technology installs in minutes with no Panel Reprogramming;** NO additional power supply & NO extra conduit. Dual Path Cell/IPs now with EZ-Connect Telco jacks & self-supervised w/o modules
- **Improve alarm response times when seconds matter most, with StarLink Fire® cellular reporting to any Monitoring Station you choose**
- **Proven to Save $1000's of Annual Budget Dollars vs. Leased Landlines –** Each Starlink Fire Cell Communicator replaces 2 POTS landlines per Fire Alarm Panel
- **AHJ-Friendly & Code Compliant: NFPA 72 2019, UL 864 10th Ed, CSFM, LAFD, NYC FD**
- **Proven to work, even where others won't. AT&T or Verizon StarLink Cellular models** all feature Signal Boost™ & twin dual diversity antennae for max. signal acquisition & null avoidance, *not possible with single stick antenna radios*
- **ALSO Integrated FireLink System: FACP with StarLink Cell or Cell/IP Built In-** Up to 32 Cloud-Programmable Zones & Onboard Annunciator; All-in-One Award-Winning Low Cost FACP/Cellular Solution

StarLink Fire

1.800.645.9445 • www.StarLinkFire.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.

For product info #21 securitymgmt.hotims.com