Issue & Beyond

- **Terrorism**
  Dealing with militants released from prison.

- **Cybersecurity**
  Companies call for privacy regulations.

- 30 **SAFER SCHOOLS**

- 40 **LEADERSHIP**

- 42 **TRAVEL SAFETY**

- 46 **#METOO INVESTIGATIONS**
NOW $800 MILLION
RUN RATE

APPROX. 30,000 EMPLOYEES
IN 320 OFFICES
Last month, I asked you to keep a secret about a “deal” that would be a game-changer for us. Well, now I can give you a hint.

SecurAmerica has just acquired controlling interest in DGS, a national security and aviation services company owned by a major airline. The airline is retaining a minority stake; they have been and will continue to be a great partner since January 1980. They have helped me to go global before and will do so again.

DGS has $450 million in revenue, has 20,000 employees, and services over 170 airports across the United States, including Alaska and Hawaii, Guam, and the Bahamas. Now we can compete with the Big Four (I mean, the Big Three).

After our deal with DGS, we now have over 30,000 employees with over 320 offices across the country. As a potential customer, why is this important? We now can compete on a national basis (and eventually, a global basis), but more importantly, we are in business for the long haul. We are not for sale. We must give you better service and for less money. Private equity is fairly predictable; they are focused on shareholders, not customers, and in general, they want to sell and reap as much profit as possible in 3 to 5 years. Our mindset is SERVICE, SERVICE, SERVICE. Their mindset is CUT, CUT, CUT and SELL. So who do you want to manage your security?

If you have questions, call me and let’s talk; my office line is 404-926-4202.
Axis network speakers are complete high-quality audio systems in a single unit. And because they're based on open standards, they're easy to integrate with other systems. Our ceiling and cabinet speakers are perfect for public address systems in educational facilities. With our horn speaker, you have a cost-efficient way of deterring intruders on campus by integrating it with your video surveillance solution in outdoor settings.

Learn more about our network audio systems at www.axis.com/products/audio
(2.5 quintillion) Bytes of data generated by Internet users every day. Vast data growth is expected in the future. PAGE 26

25 Approximate number of Americans jailed for terrorist activity expected to be released by 2021. PAGE 20

“We’re in the middle of the mediation, this girl flips out—next thing I know, she and I are both through the sheetrock wall in the assistant principal’s office.”

School Resource Officer Kevin Wren, describing an incident with a student he later helped graduate on time. PAGE 31

$3.6M Amount paid by Sherwood Food Distributors, plus other relief, to settle a class sex discrimination lawsuit filed by the U.S. Equal Employment Opportunity Commission. PAGE 56

Security Management (ISSN 0145-9406) Volume 63, Number 1, is published monthly by ASIS International, 1625 Prince St., Alexandria, VA 22314; 703.519.6200; fax: 703.519.6299.

Subscriptions: ASIS members—$60 for 1 year (included in dues, non-deductible). Nonmembers in US, Canada, and Mexico—1 year, $60; 3 years, $62. 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 © 2019 ASIS International, Inc. This information is protected by copyright and trade mark laws under U.S. and International law. No part of this work may be reproduced without the written permission of ASIS International. Statements of fact and opinion are made on the responsibility of the authors and do not imply an opinion on the part of the editors, officers, or members of ASIS. Advertising in this publication does not imply endorsement or approval by Security Management or ASIS. The editors reserve the right to accept or reject any article or advertisement. Quantity reprints of 100 or more copies of each article may be requested from Security Management Reprints Dept. at 703.518.1451.
WHEN ONE DOOR CLOSES, ANOTHER OPENS.

INSTALLED IN FACILITIES GLOBALLY, STRIKEIT INTEGRATES WITH HIGH IN-RUSH PANIC BARS, LOW CURRENT MLR EXIT DEVICES, ELECTRIC STRIKES AND MAG LOCKS. PROVEN POWER AND PRECISE FUNCTIONALITY COUPLED WITH AN UNPARALLELED WARRANTY, EQUALS RELIABLE ACCESS 24/7.

ALTRONIX SECURES YOUR MOST CRITICAL INS AND OUTS.
JANUARY 2019

**CONTENTS**

**FEATURES**

**COVER STORY**

**30**

**RESOURCESFUL RELATIONSHIPS**

School resource officers are going above and beyond traditional law enforcement duties to build relationships with students, inspire educational growth, and prevent threats.

*By Holly Gilbert Stowell*

**X34**

**VIOLENCE MITIGATION**

**GUIDANCE ON THREAT ASSESSMENT TEAMS**

The U.S. Secret Service offers a baseline process for establishing a team to prevent potential violence in schools.

*By Cody Mulla, CPP*

**X40**

**LEADERSHIP**

**SERVING THE NEW GENERATION**

ASIS President Christina Duffy, CPP, shares her thoughts on building a security career, and the value of connecting through ASIS.

*By Security Management staff*

**X42**

**TRAVEL SAFETY**

**A GLOBAL SAFETY PLAN PROTECTS CORPORATE TRAVELERS**

Keeping employees safe while they travel means more than just a number to call in an emergency.

*By Lilly Chapa*

**X46**

**INVESTIGATIONS**

**HOW TO INVESTIGATE #METOO**

A proper investigation requires a mixture of skill, experience, and patience. The fundamental rules? Be fair, thorough, and professional.

*By Eugene F. Ferraro, CPP, PCI*
PREPARE TO ADVANCE YOUR CAREER
JOIN US IN SAVANNAH, GA.

Strengthen your knowledge of core security principles. This is the type of vital information you’ll find in our February line-up of educational programming in Savannah.

CPP Review Program
25-26 February
Benefit from an accelerated, high-level overview of the security concepts and practices assessed on the Certified Protection Professional (CPP®) exam so you can develop a personalized study plan.

PSP Review Program
25-26 February
Intended to supplement your other certification exam preparation activities, this program provides a high-level overview of the three key domains assessed on the Physical Security Professional (PSP®) exam.

Assets Protection Course™:
Principles of Security (APC I)
25-28 February
You can’t advance in the profession without a strong foundation. Make sure your fundamental knowledge of assets protection and its universal principles is rock-solid by attending APCI!

Reserve your hotel by 4 February
Learn more and register at asisonline.org/profdev

WEBINARS

SUBSCRIBE NOW FOR 2019 AND SAVE!
With a webinar subscription, you’ll gain access to all live and on-demand webinars for 2019—a minimum of 20 programs on key and trending topics such as active assailant, security operations, ESRM, management and leadership, and more. Not a subscriber? Single webinars: $49 member, $79 nonmember.

FREE Informational Webinar
REACHING YOUR CAREER POTENTIAL:
WHY ASIS CERTIFICATIONS ARE A VITAL PROFESSIONAL INVESTMENT
15 January 2019 @ 3:00 pm ET

Register today!
THE PRIVACY PROBLEM
Private companies come together to demand that authorities create privacy regulations to protect users’ data and technology.

By Megan Gates

THEORY MANAGEMENT
EDITORIAL STAFF
Teresa Anderson
editor-in-chief
Teresa.Anderson@asisonline.org

Mark Tarallo
senior editor
Mark.Tarallo@asisonline.org

Megan Gates
associate editor
Megan.Gates@asisonline.org

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

PRODUCTION & CREATIVE SERVICES STAFF
Tyler Stone
art director
Tyler.Stone@asisonline.org

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

Caitlin Donohue
graphic designer
Caitlin.Donohue@asisonline.org

Molly Fu
graphic designer
Molly.Fu@asisonline.org

Mariah Bartz
graphic designer
Mariah.Bartz@asisonline.org

Matthew Kreider
publishing specialist
Matthew.Kreider@asisonline.org

Pam Fischer
advertising production specialist
Pam.Fischer@asisonline.org

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

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

CONTENTS

10 CONTRIBUTING AUTHORS

12 SM DIGITAL

14 EDITOR’S NOTE
Finding joy.

16 NEWS & TRENDS
First responders face layers of risk.
By Mark Tarallo

20 NATIONAL SECURITY
Some 9/11-era terrorists will be released from prison soon.
By Lilly Chapa

24 CASE STUDY
Situational awareness and mass notification protect employees.
By Holly Gilbert Stowell

52 ASIS NEWS
Meet the ASIS Board Management Committee.

53 ASIS BOARD OF DIRECTORS

56 LEGAL REPORT
Courts rule on arbitration and discrimination; legislators act on cybersecurity and supply chains.
By Megan Gates

60 INDUSTRY NEWS

62 MARKETPLACE
Cabinet locks and other new products.

65 ADVERTISER INDEX

66 FLASHBACK
April, 1965

CHECK OUT MORE ONLINE at
www.securitymanagement.com
CODY MULLA, CPP
DIRECTOR, SECURITY RISK MANAGEMENT
HILLARD HEINTZE

Cody Mulla, CPP, is an expert in emergency and crisis management. He is finishing his Ph.D. in Organizational Development and holds master’s degrees in Human Resource Development/Lean Six Sigma; Industrial Organizational Psychology; and Leadership and Crisis Management. He holds certifications from several organizations, including the International Association of Emergency Managers and the Texas Commission on Law Enforcement. Mulla serves on the ASIS School Safety and Security Council and the Utility Security Council.

“Guidance on Threat Assessment Teams”
PAGE 34

EUGENE F. FERRARO, CPP, PCI
CHIEF EXECUTIVE FORENSICPATHWAYS, INC.

A former Marine Corps naval aviator and combat flight instructor, Gene Ferraro, CPP, PCI, is board certified in human resources management and is a Certified Fraud Examiner. He has been a member of ASIS since 1987 and serves on the ASIS Standards and Guidelines Commission. He co-chaired the technical committee that developed the national ANSI/ASIS Investigations Standard.

Ferraro is also an inventor with three new patents; a licensed investigator in California, Colorado, and Illinois; and the author of 15 books.

“How to Investigate #MeToo”
PAGE 46

THOMAS J. RZEMYK | UNIVERSITY PROFESSOR
Dr. Thomas Rzemyk serves as a university professor and course curriculum writer at multiple institutions across the United States. He is a renowned international speaker, educational researcher, college lecturer, and academic writer. Rzemyk has presented research at prestigious conferences across the globe. He has written several articles, papers, and book chapters, as well as two cybersecurity textbooks that will be released in 2019 and 2020.

Book review PAGE 17

DANIEL BYLES | SECURITY AND CRISIS MANAGER
Dan Byles is an organizational resilience practitioner with international experience in risk, security, emergency, crisis, and continuity management. As an officer in the Australian Defence Force, he undertook operations and logistics management roles within multinational missions and coordinated regional engagement, population security, and humanitarian assistance initiatives in response to disasters around the world. He is a member of the ASIS Cultural Properties Council and the ASIS Global Terrorism, Political Instability, and Transnational Crime Council.

Book review PAGE 22

DECLAN GARRETT | HEAD OF SECURITY UNIT | LOUVRE ABU DHABI
Dr. Declan Garrett is responsible for the security of the art collection of the Louvre Abu Dhabi. He is a visiting lecturer to the Berlin Institute of Economics and Law, where he teaches in the master’s program in International Security Management. Dr. Garrett serves on the ASIS International Cultural Properties Council, chairing the Museum Committee. He is the director of Academic Research at the Security Institute of Ireland and the academic representative to the national security regulator.

Book review PAGE 28

KHALID A. AL-GHAMDI, CPP, PSP | SECURITY SUPERINTENDENT | SAUDI ARAMCO
Khaled Al-Ghamdi, CPP, PSP, graduated from Bucknell University with a Bachelor of Science degree in Electrical Engineering. He has worked for Saudi Aramco since 2000, and he currently leads the security engineering division of the company. Al-Ghamdi has been a member of ASIS since 2010 and is active in the Dhahran Chapter. He was recently appointed to the ASIS Professional Certification Board.

Book review PAGE 54
Call for Presentations
NOW OPEN

Share your expertise and experience with an exclusive audience of security management practitioners looking for cutting-edge strategies and best practices to help secure their organizations and communities.

SUBMISSION DEADLINE: JANUARY 31, 2019

Learn more and submit your proposal today!
GSX.org/CFP
First Responders
A report finds that law enforcement personnel and firefighters are more likely to die of suicide than in the line of duty.

Risk Management
Deloitte consultants surveyed CEOs and board members on how leaders can improve their risk management.

Privacy
Intel released a draft bill for the United States designed to optimize innovation and protect privacy.

School Resource Officers
The National Association of School Resource Officers offers best practices and recommendations for agencies involved in policing schools.

First Responders
A report finds that law enforcement personnel and firefighters are more likely to die of suicide than in the line of duty.

Risk Management
Deloitte consultants surveyed CEOs and board members on how leaders can improve their risk management.

Privacy
Intel released a draft bill for the United States designed to optimize innovation and protect privacy.

School Resource Officers
The National Association of School Resource Officers offers best practices and recommendations for agencies involved in policing schools.
Every company faces risk that is unique to the complexities of their business. G4S can help you identify what those are through our Security Risk IQ Survey. Developed in conjunction with Georgia State University, the survey is a free online questionnaire that helps security professionals identify and quantify the risks they face. In just a few minutes, you can be better prepared for future threats.

Take a FREE Security Risk IQ survey. Visit SecurityRiskIQ.com

The one complete force in security. | 888-645-8645 | www.G4S.us

For product info #6 securitymgmt.hotims.com
As a culture, we are obsessed with the pursuit of happiness, but in the process we overlook joy,” says designer Ingrid Fetell Lee in her TED Talk: “How Can We Design More Joy Into Our Surroundings?” Happiness is a long-term state of being, but joy occurs completely in the moment. It is giddy and infectious and, Lee argues, vital to our well-being.

The feeling of joy may be elusive, but we can access it through aesthetics, through design. Joyful aesthetics change people’s attitudes and behavior. “And they help us understand why one environment makes people anxious and competitive, while another brims with sociability and tolerance,” writes Lee in her new book Joyful.

Joy is particularly lacking in the public spaces we seek to protect, particularly schools—the topic of this month’s cover story. Lee relates how the work of the nonprofit Publicolor affects underserved public schools in New York City. These schools were industrial institutions constructed with concrete and adorned with a tan and taupe color scheme. Publicolor enlists students to repaint the schools in bright, vibrant colors as part of its program to engage at-risk youths.

Though empirical evidence is scarce, the repainted schools report improved attendance from staff and students, a drastic reduction in graffiti, and better test scores. Perhaps most surprisingly, both teachers and students “consistently say they feel safer in a school that has been painted by Publicolor,” writes Lee.

Another example of joyful design that advances security objectives is the new Sandy Hook Elementary School. After the 2012 shooting, the school was torn down and rebuilt. The new bright, colorful, and spacious building has a secret.

According to an article by Chris Weller in Business Insider, the new open design works hand-in-hand with security. Students and visitors “pass through multiple security checkpoints on the way to the entrance,” writes Weller. “They also pass by several bioswales, which are angled landscapes that direct storm run-off and keep outside people at a distance.”

The 20-foot windows in the colorful atrium let in abundant light and allow staff to clearly see anyone approaching the school. Each classroom has reinforced walls and bullet-resistant windows. Parents still worry about security, but Weller notes that the campus “will protect all future students in what is essentially a very safe work of art.”

This issue also boasts other reasons for joy. In the spirit of continuous improvement, Security Management has added more color, refreshed the design of the departments, and added two new items: “Flashback” explores the history of ASIS and the security industry (see the first example on page 66), and future issues will explore the lives of members through the “Getting to Know” page.

In this season of renewal and new beginnings, we can all resolve to carve out time for joy. We might be happier and healthier—not to mention safer—for it.
DETEX CUSTOMER SERVICE TECHNICIANS live and thrive in the urgent world of security door hardware. So getting your immediate questions answered is priority one. Whether you need guidance with a challenging installation, are inquiring about training or want help making a hardware decision, you can access a team with nearly five decades of combined experience. You’ll have the answers you need before you know it. Just call 800-729-3839.

DETEX.COM/IMA1

- Advantex line of exit devices & electrical functions
- Super heavy duty low energy ADA operator
- Automatically operated door easykits
- Weatherized delayed egress easykits
- Tailgate detection

LISTEN • DESIGN • BUILD • SUPPORT

For product info #7 securitymgmt.hotims.com
FIRST RESPONDERS face layers of risk. First is the possible harm during a response—being burned in a fire, hit by a bullet, or injured in a chaotic rescue operation.

Then there’s the possibility of long-term effects. Emerging seemingly unscathed from an event, responders may find at some point in the future—even years down the road—that they are now fighting a terminal disease, or a possibly fatal case of depression or addiction, that was triggered or caused by an experience they had during a response.

“They are not only putting themselves on the line. They also putting their futures on the line,” says Harry Rhulen, an emergency response expert and ASIS International member who is coauthor of the book *Disaster Ready People for a Disaster Ready America*.

Take for example the 343 firefighters and paramedics who were among the 2,753 individuals who died in 9/11 attacks on the World Trade Center. The first responders had direct exposure to the building materials and breathed in dust carrying asbestos, lead, dioxins, and other potentially harmful substances.

As of September 11, 2018, the 17th anniversary of the attacks, more than 150 of the responders had died, according to New York Fire Department estimates. Some of these deaths have been recent, and many medical experts expect the death rate to continue to rise in the future. Scientists have found that numerous cancers, such as asbestos-related cancers, can lie dormant for decades before turning deadly.

“It’s not surprising what we are seeing now, 17 years later. Cancer can take a long time to develop when it’s caused by exposure to contaminants,” Rhulen says.

Some have also raised concerns about responders who are exposed to Florida’s recent algae emergency or “red tide,” which plagued the state’s Gulf Coast last year and continues to spread. Caused by the neurotoxin-producing algae *Karenia brevis*, the red tide has killed thousands of fish, released noxious fumes, and forced widespread beach closures. Studies have associated the recent occurrence of this tide with increases in nearby medical facility visits for respiratory issues.

Moreover, besides the disasters themselves, the way that first responders are now used is also increasing their risk, Rhulen says. “They are being sent in more and more often, and more rapidly than ever before,” he explains. He offered the example of active shooter response. In the past, first responders would gather on the perimeter; now, they are expected to immediately seek out the shooter, which increases their risk.

And besides the physical health challenges, first responders also face long-term mental health risks, experts say.

A recent white paper issued by the Ruderman Family Foundation found that first responders (policemen and firefighters) are more likely to die by suicide than in the line of duty. The study found that there were at least 140 police officer suicides and 103 firefighter suicides in 2017. In comparison, 129 police officers and 93...
**People who are exposed to catastrophe vary in the limits and amount of impact on their psyches. Each individual is different.**

firefighters died in the line of duty the same year. The suicides were the result of mental illness, including depression and post-traumatic stress disorder (PTSD), which stemmed from constant exposure to death and destruction, the study found.

“First responders are heroes who run towards danger every day in order to save the lives of others,” said Jay Ruderman, president of the Ruderman Family Foundation, in a statement. “They are also human beings, and their work exerts a toll on their mental health.”

Rhulen, who echoes Ruderman’s statement, says that first responders who experience disasters “have a new normal afterward—they are not the same. People are permanently changed by the experience.” But it’s usually impossible to predict the extent and seriousness of the after-effects, he adds. “People who are exposed to catastrophe vary in the limits and amount of impact on their psyches. Each individual is different,” he explains.

That each-individual-is-different sentiment also holds true during the response itself, he says. Often, “unsung heroes” will emerge from the crowd in a disaster or crisis, such as an ordinary citizen who is not a first responder but will still act bravely and effectively. “It’s the ones you never expected who come forward and are ready to perform,” Rhulen says.

And like a cancer that may only emerge after years of dormancy, trauma can be submerged and repressed by the responder, only to emerge years later, says Dr. Judith Kuriansky, a clinical psychologist who was “in the pit” at the bombed-out World Trade Center on 9/11 as a first responder providing psychological aid. She also worked at the site’s family assistance center.

“Any kind of abuse or trauma that is being submerged and repressed can emerge, even 30 years later,” she says. “Trauma gets locked in the body, neurologically, and it can be retriggered.”

For a highly publicized event like the 9/11 attacks or a mass shooting, it is possible for the public commemoration of event anniversaries to retrigger these bad experiences, so it’s possible first responders will suffer during those times, Kuriansky explains. However, for other first responders, such commemorations can have a healing effect, with people gathering, sharing experiences, and honoring victims in memorials, and whole communities coming together.

There are other practices that can help first responders, experts say. For example, training can mitigate the traumatic response to a crisis. Activities like response exercises and drills can help prepare the worker’s mind for experiencing disasters, so that the event itself has precedent, Rhulen says. At least one study of first responders has shown that those with training and preparation “tend to fare

**SECURITY ECONOMICS**

BY MARKO CABRIC. Butterworth-Heinemann; Elsevier.com; 240 pages; $99.95.

**SECURITY IS VITAL** to all organizations, regardless of whether their goal is to earn a profit. The cost of running security in a corporate environment can be very high. From Corporate Security to Commercial Force: A Business Leader’s Guide to Security Economics highlights the importance of running an economical yet effective security program, and it explains how security can add to the bottom line. It also offers theoretical ways to measure the impact of incident losses.

Author Marko Cabric is a global practitioner, consultant, and academic with decades of corporate security management and government experience. That experience lends validity, clarity, and substance to complex topics such as corporate security and economics in an era of global changes.

The book is divided into five sections that lead the reader through the author’s theories of security economics. “Conceptualize” covers the history and philosophies of security and economics. “Reevaluate” discusses how to understand security incidents and quantify information security. “Embrace” outlines the importance of efficiency and the challenges of outsourcing security in corporate environments. “Utilize” focuses on resilience and strategies for marketing security in an organization. The final section, “Organize,” outlines the importance of metrics and emerging technologies.

There are two specific shortcomings of this book. First is the lack of case studies, which could offer the reader the opportunity to apply the principles and theories to real-world scenarios. The second shortcoming is a failure to provide traditional formulas, statistics, and figures to quantify the theoretical statements. When discussing economics, quantitative data and formulas are essential.

Ultimately, the book is well-written, researched, and presented. It is a great addition to security management literature and a scholarly asset. Each chapter provides discussion and self-assessment questions that encourage the reader to reflect on the material. Undergraduate institutions will value it for its brief theoretical views on the economic benefits of security in the corporate sector. Financial administrators and security practitioners in the public and private sectors can also learn from it.

**REVIEWER:** Thomas Rzemyk, Ed.D., is director of technology and cybersecurity instructor at Mount Michael Benedictine School. He is a criminology discipline reviewer in the Fulbright Scholar Program.
better after the fact” in terms of their mental health.

Emotional management is another type of valuable training for first responders, Kuriansky says. This helps the responder to better understand the different manifestations of stress and trauma and how they react to it.

HATE CRIMES

Victims who reported hate crimes in 2017 were primarily targeted due to racial/ethnic bias.

Hate crime incidents reported by bias:

- **59.6%** Race/Ethnicity
- **20.6%** Religion
- **15.8%** Sexual Orientation
- **4.1%** Other

**SOURCE:** Hate Crime Statistics, 2017, FBI, November 2018

They will learn their personal stress symptoms and what is effective in dealing with them, such as exercising and talk therapy.

For coworkers, friends, and family members who want to help first responders deal with these difficult situations, Kuriansky says that it is helpful to know their coping style. Some people are talkers, who benefit from discussing their feelings, and some are doers, who find it best to busy themselves in activity, she explains. And it’s best not to pressure any responder in talking, but advisable to tell them that, “If you have anything you ever want to talk about, I’m here to listen.”

Overall, helping first responders is an important global issue as well, explains Kuriansky, who has been a responder providing psychological aid in regions all over the world, ranging from the Middle East to the Caribbean. Knowing the responder’s coping strategy is important in every region, and it can sometimes be related to cultural or religious beliefs, she explains.

She offered an example from her work in Haiti. A first responder who is very religious might have an attitude of whatever happens is predetermined, because it is “God’s will.” That person’s method of coping may be centered around prayer and keeping faith strong, so assistance techniques can be shaped around this central pillar. “It affects the way you approach them,” she says.

**STRATEGIC RISK**

Strategic risk assessment is becoming a crucial practice for an increasing number of companies. Seeking some best practices, Deloitte consultants surveyed 200 CEOs and 200 board members on how leaders and managers can improve their risk management capabilities.

Almost all respondents in the Deloitte study—95 percent of CEOs and 97 percent of board members—said they believed their organizations would face serious threats or disruptions in the next two to three years.

Diving in deeper, the survey asked respondents which types of threats would pose the most risk to their organization’s growth. The two most serious threats were new disruptive technology (cited by 35 percent of respondents) and cyberattacks (27 percent). The other top threats cited were the organization’s key business partners (26 percent), brand or reputational damage (24 percent), and an unhealthy organizational culture.

In general, the study found that “leaders tend to focus on current, isolated, tactical risks rather than emerging strategic risks. And they generally take reactive rather than proactive measures,” according to the report. The survey responses revealed that many organizations are falling short in these areas: investment in technology that aligns with strategy, engagement from
board members and senior management, and alignment of risk and risk officers within an organization.

The study also examined risk in four crucial areas of the operations: cyber and technology, extended enterprise (such as working with third-party vendors), culture, and brand/reputation.

For example, in the cyber sector, although most respondents believed cybersecurity was a major concern, only 30 percent of the CEOs and board members combined described themselves as highly engaged in the area. The study recommends that more CEOs and board members should be engaged in dealing with this risk.

“Increasing dependence on technology calls for more intensive leadership engagement through such practices as war-gaming participation, scenario planning, threat intelligence reviews, and a basic understanding of advanced analytics,” the report says.

Too often, the study found, companies manage cyber risk by doubling down on technology. “They believe a tech-centric threat calls for tech-centric investments,” the report says. Instead, business leaders should take a broader and more integrated view, and consider strategic risk through the lens of governance, talent, and reputation, and how it might affect these areas of operations.

In general, the study recommended the following practices to leaders to stay ahead of the curve: Proactively position the organization so that it can address significant risks; apply the right technology to risk data, insights, and predictive analytics; adopt integrated risk reporting and governance; and establish CEO and board member alignment to drive informed decisions.

“Leaders who manage strategic risks effectively are better able to navigate disruption, accelerate performance, and gain competitive advantage,” the study says.
ILLUSTRATION BY L.J. DAVIDS

NATIONAL SECURITY | TERRORISM

BATTLEFIELD IN THE MIND

SOME 9/11-ERA TERRORISTS WILL BE RELEASED FROM PRISON SOON—AND A LOT HAS CHANGED IN THE TERRORISM LANDSCAPE DURING THAT TIME. BY LILLY CHAPA

FOLLOWING THE SPIKE in terrorism activity and related convictions over the past two decades, a new national security challenge is rapidly approaching: the release of dozens of terrorists from prisons around the world. Sentencing those involved in extremist activity is notoriously challenging. It often relies on unrelated criminal convictions or the charge of providing material support to a terrorist organization, which results in sentences of 13 years on average. This means that those convicted in the years following 9/11 are approaching their release date.

In the United States, about 25 Americans charged with terror crimes are expected to be released by 2021, and that number will jump to 72 in 2025. At least 80 terrorists will be released by the end of the year in the United Kingdom, and the first man to be convicted in connection with 9/11—a Moroccan man living in Germany—was released from prison in 2018.

“If you go to jail, it doesn’t mean you’re not a terrorist when you come out,” said Michael McGarrity, assistant director of the FBI’s counterterrorism division, during a session at GSX 2018. While the soon-to-be-released prisoners may be monitored, there is currently no way to track those convicted of terror-related crimes—legislation establishing a national database has continually stalled. And, according to Jennifer Hesterman, a retired U.S. Air Force colonel and vice president of business resiliency and education services at Watermark Risk Management International, LLC, there are no effective deradicalization programs within the prison system.

“The people from 9/11 are coming out of prison in the next couple years, and they have not been rehabbed. It’s a concern to me,” Hesterman said during another GSX 2018 session. “They are coming back out and we can’t keep track of them; we don’t have the resources. We’re not actively trying to work with them and train them to go the right direction.”

A lot has changed in the terrorism landscape over the past decade, and both Hesterman and McGarrity said counterterrorism efforts are struggling to keep up with the rapid evolution of recruitment, detection, and communication techniques between terror organizations and potential extremists around the world. While McGarrity said extremist recidivism rates tend to be low following a prison stint, it is challenging to detect and act on concerns about further radicalization.

“Never before have we seen so many individuals inspired and willing to take direct actions,” McGarrity said. “We’ve arrested more subjects over the past two years—many times we have to arrest them on nonterrorism charges, whatever it is to take that person off the street before they commit an attack. We’ve consistently arrested 100-plus people a year since 2015. We have seen how the message has evolved. ISIS encourages and empowers them to take action on their own, and anyone is a worthy target.”

The top terror threat to the United States continues to be homegrown...
violent extremists—those who are recruited and radicalized online.

“Radicalization is online—there are far too many subjects in the U.S. being radicalized online in their basements,” McGarrity noted. “These aren’t tough people who went to training camps. They were radicalized online, socially awkward, and are not meeting mentors or other operatives.”

Hesterman outlined the methods used to radicalize individuals and described the people who tend to fall prey to such efforts. There are two types of lone actors, she said—one that is well-adapted to society and makes the choice to leave society, and another is not well adapted, and society leaves them.

“I’ve seen cult of jihad up close and personal, and it’s powerful,” Hesterman said. “They know how to hook people, target the message to the audience. They’ll use rap music for teenagers or target the message to professors. They have people all day online looking for disgruntled people they can seek out. They isolate them—don’t tell anyone we’re having this discussion—then they encourage them. This is a long process, but the people in the violent ideology business, they are patient.”

It can be exceedingly difficult to identify potential homegrown extremists due to the nature of online-only radicalization and encrypted communications platforms. Additionally, there’s no one demographic that is especially susceptible to radicalization—previous homegrown extremists have tended to be male and 19 to 25 years old, but that number is trending lower. Hesterman showed instances of extremists who target children through English-language workbooks that use jihadist beliefs as examples, and McGarrity pointed out several occasions in which teenagers attempted to plan jihadist-inspired attacks.

McGarrity also noted that teenagers can be especially susceptible to jihadist influence due to the violent aspect of it—and that can make it difficult to know what role the ideology plays in their radicalization.

“Teens are more attracted to violence than propaganda,” McGarrity explained. “Ideology can be a source of inspiration, but they are motivated to act in violence. We had one subject who said the reason why he wanted to kill others was that he was inspired by ISIS, Hezbollah, and the white supremacy movement. Is that someone who’s really a stalwart educated in the ideology that he’s following, or someone looking to commit violence?”

However, violence isn’t the only threat. Both McGarrity and Hesterman emphasized the role that nonviolent
extremists can play in the radicalization and terrorism landscapes.

“We’re struggling with this area—radical preaching, writing, or think tanks,” Hesterman noted. “What we do is give them platforms because we think it will let off steam if a group is going to boil over—we think that’s a vent—but they’re still able to get their message out. A group crosses a line when they do not further peace or harmony in society. If that line is crossed, they are recruiting. This is hard, because there are legitimate groups that cross that line.”

McGarrity agreed, noting that the threat of so-called “keyboard warriors” who never set foot on a battlefield cannot be discounted. Samir Khan, a Pakistani American living in North Carolina, was recruited to become the editor and publisher of the English-language Inspire magazine, writing articles such as “Make a Bomb in the Kitchen of Your Mom” out of his parents’ basement.

To combat the ever-evolving threat, McGarrity said it is more important than ever for the FBI to work with state and local law enforcement officials, as well as the private sector.

“The bystander is one of the most important tools in our fight against terrorist attacks,” McGarrity said. “The human intelligence community is important. We get about 15,000 tips a year and rely on partnerships with state and local law enforcement to sound the alarm.”

Joint terrorism task forces—the approximately 150 groups across the country that combine intelligence officials and counterterrorism specialists to fight radicalization in their communities—are key to community cooperation, McGarrity said. “If we did it alone, we would not be successful,” he said.

When it comes to the private sector, the FBI wants to provide learning in targeted sectors to understand the threats they may be able to identify. “The CSO is not who needs that training,” McGarrity noted. “We need to work with people on front lines. The more we can tell them about threats and what to look for, we get better leads. From the retail and transportation sectors, leads have been incredible—we get thousands.”

Hesterman said that deradicalization—which is especially important now that extremists are leaving prisons and coming back from the front lines in Iraq and Syria—has a long way to go.

“If we tell people their ideology is wrong, we have to tell them what is right, and how to replace that,” she said. “We have to offer an alternative, and that’s hard for us. That’s a huge dilemma. It’s hard for us to argue with them because they have taken the bait. If they think their beliefs or way of life are under attack, they lash out.”

Both McGarrity and Hesterman argued that, despite the shrinking numbers of ISIS in Syria and Iraq and the seemingly low profile of al Qaeda groups, the terror threat remains critical. And the impending release of radicalized individuals from prison is a stark reminder of that.

“The war on terror is not ending any time soon,” Hesterman concluded. “We’ve been able to dislodge ISIS in geographical areas, but the battlefront is the mind, and ideology is the glue holding this together. Terrorism isn’t geographically somewhere—it’s a battle of ideas. We’re part of the environment and problem, and what we do impacts this situation. Humility is a powerful tool in this fight.”

**PERSONAL SECURITY**

BY RICHARD BRADFORD. CreateSpace; amazon.com; 182 pages, $9.99.

NOW MORE THAN EVER, the reach of terrorist attacks highlights the importance of personal readiness. Soberly, Personal Security: Preparing for the Unexpected in an Era of Crime and Terrorism asserts that a typical individual’s chances of evading or countering a violent attack are poor. That’s because people are often unsuspecting, unprepared, and unfamiliar with their security environment.

With a primary focus on threat avoidance, this book explains how to identify and manage personal security risks where they often appear—in transit. Author Richard Bradford provides principles that can help individuals understand and adjust to their security environment. Covering topics such as travel route analysis, observation skills, situational awareness, surveillance detection, and vehicle driving, clear and actionable guidance is provided to readers on how to identify threats, understand what they mean, and respond before the threat can materialize. To help contextualize the threat, Bradford expertly explains the stages of a violent attack from preparation to execution, taking the reader into the mind of a terrorist.

At its core, the book seeks to reduce complacency and harness the power of habit in embedding effective risk-avoidance behavior through practice and repetition. Bradford convincingly argues that the power of habitual, pre-incident analysis is more potent than counterattack measures such as martial arts and weapons, noting that these measures require skills that inherently deteriorate during a high-stress, low-familiarity situation. Avoidance skills are easier to learn and apply—and more likely to enable safety when compared with countering techniques.

While the book provides crucial advice for those susceptible to modern terrorism, it also provides an expert reference for practitioners who must translate security theory into meaningful practice in the wider community. Candid and authoritative, Personal Security is a valuable guide for security professionals seeking to engender the serious use of proven personal security treatments by those at risk of violence.

**REVIEWER:** Dan Byles is a former Australian Army Officer who served in the Middle East and Afghanistan. He leads security, business continuity, and crisis management programs in the higher education, business, and government sectors. Byles is a member of the ASIS Cultural Properties Council and the Global Terrorism, Political Instability, and Transnational Crime Council.
ASIS EUROPE 2019
FROM RISK TO RESILIENCE
27–29 March
Rotterdam, Netherlands

www.asiseurope.org
NATIONAL OILWELL VARCO USES SITUATIONAL AWARENESS AND MASS NOTIFICATION PLATFORMS FROM EVERBRIDGE TO COMMUNICATE WITH EMPLOYEES AND PROVIDE ASSISTANCE.

BY HOLLY GILBERT STOWELL

With approximately 1,000 employees traveling globally in any given month, National Oilwell Varco (NOV), an oilfield equipment manufacturer, prioritizes protecting its workers. “From a security perspective, our challenge is to ensure that our employees are safe as they go out and meet our diverse customer needs,” says David Dadd, travel security manager and global security operations center (GSOC) manager at NOV.

The company, which has more than 600 facilities and 35,000 employees around the world, produces oilfield equipment, including offshore and deep-water rigs, for customers all over the map. NOV employees are routinely sent to service that equipment and provide support at various locations. “Our largest presence is in the United States, but we also have a presence in South Africa, Central America, Africa, Europe, the Middle East, Asia, and South America,” says Bob Bernazal, director of security at NOV. “We do a lot of predictive analysis inside our GSOC to ensure that as our workforce travels, they are not traveling into harm’s way.”

The GSOC gives NOV a precise picture of where its employees are located at any given time, with analysts reviewing real-time information on threats and any potential risks around the globe. “We use a risk rating to see what kind of risk level there is in that environment,” Bernazal says. “That entails a multitude of things—whether they need geolocation services, or what type of security that’s going to be required by the third party. So, it allows us to properly understand the environment and the risk management techniques that we need to apply to the situation.”

NOV’s security program doesn’t just look after travelers on foreign soil. The company’s risk management program is designed to protect employees at home, too.

When an F5 Tornado hit Moore, Oklahoma, in May 2013, killing 24 people and injuring more than 200, NOV wanted to garner situational awareness of where its workers were located. Though none of its workers were among those killed, NOV provided a company-funded hotel room to employees in need of assistance. “Unfortunately NOV was hit pretty hard when the F5 tornado went through Oklahoma,” Bernazal says. “We went through this initial process of just trying to understand where people were located, which was hard from a multinational company perspective.”

While NOV was already taking measures to safeguard its employees, Dadd notes that this incident led to improvements in its security systems by incorporating assets, employees, and travelers worldwide.

NOV adopted a tool called Visual Command Center from IDV Solutions in the summer of 2014 to track and monitor company assets, both domestically and abroad. “We had one half of the puzzle solved, and the other half of that puzzle was trying to communicate directly with our affected employees,” Bernazal notes.

When IDV Solutions was acquired by Everbridge in January 2017, NOV decided to employ Everbridge’s

PHOTO COURTESY OF NOV

CASE STUDY | CRISIS COMMUNICATIONS

WELLSPRING OF SAFETY

With approximately 1,000 employees traveling globally in any given month, National Oilwell Varco (NOV), an oilfield equipment manufacturer, prioritizes protecting its workers. “From a security perspective, our challenge is to ensure that our employees are safe as they go out and meet our diverse customer needs,” says David Dadd, travel security manager and global security operations center (GSOC) manager at NOV.

The company, which has more than 600 facilities and 35,000 employees around the world, produces oilfield equipment, including offshore and deep-water rigs, for customers all over the map. NOV employees are routinely sent to service that equipment and provide support at various locations. “Our largest presence is in the United States, but we also have a presence in South Africa, Central America, Africa, Europe, the Middle East, Asia, and South America,” says Bob Bernazal, director of security at NOV. “We do a lot of predictive analysis inside our GSOC to ensure that as our workforce travels, they are not traveling into harm’s way.”

The GSOC gives NOV a precise picture of where its employees are located at any given time, with analysts reviewing real-time information on threats and any potential risks around the globe. “We use a risk rating to see what kind of risk level there is in that environment,” Bernazal says. “That entails a multitude of things—whether they need geolocation services, or what type of security that’s going to be required by the third party. So, it allows us to properly understand the environment and the risk management techniques that we need to apply to the situation.”

NOV’s security program doesn’t just look after travelers on foreign soil. The company’s risk management program is designed to protect employees at home, too.

When an F5 Tornado hit Moore, Oklahoma, in May 2013, killing 24 people and injuring more than 200, NOV wanted to garner situational awareness of where its workers were located. Though none of its workers were among those killed, NOV provided a company-funded hotel room to employees in need of assistance. “Unfortunately NOV was hit pretty hard when the F5 tornado went through Oklahoma,” Bernazal says. “We went through this initial process of just trying to understand where people were located, which was hard from a multinational company perspective.”

While NOV was already taking measures to safeguard its employees, Dadd notes that this incident led to improvements in its security systems by incorporating assets, employees, and travelers worldwide.

NOV adopted a tool called Visual Command Center from IDV Solutions in the summer of 2014 to track and monitor company assets, both domestically and abroad. “We had one half of the puzzle solved, and the other half of that puzzle was trying to communicate directly with our affected employees,” Bernazal notes.

When IDV Solutions was acquired by Everbridge in January 2017, NOV decided to employ Everbridge’s
Critical Event Management (CEM) platform alongside Visual Command Center. CEM includes a mass notification tool that pushes out messages to employees in the event of an emergency or incident affecting the company. Employees can choose whether they want to be notified by text, email, or phone, and their order of preference. Workers can also communicate to the company by sending a message back through the Everbridge app or their preferred device.

When Hurricane Harvey struck the southern United States in the summer of 2017, the Everbridge platform was put to use immediately. “We started tracking Hurricane Harvey through the Visual Command Center, which showed the predictive storm path in relation to our assets,” Bernazal says. “So, we were able to tell the senior managers in the company down to the facility managers that, ‘Yes you are indeed in the storm path.’”

Rising floodwaters prevented workers from going to most of NOV’s Houston locations, so the organization used Everbridge to send notices to affected employees about whether to come into work, as well as gather information on who needed assistance. “We used the mass communication tool to communicate to our Houston-based workforce to say, ‘Do you need assistance?’” Bernazal explains. “Then when they started communicating back to us, we began directing company resources to help those affected by the storm.”

NOV provided resources for its employees whose homes and communities were hardest hit by the storm. “They were deeply grateful that the company would invest not just time and resources in them, but send crews out to their homes to help them in their time of need,” he says.

Another problem was that the security and crisis management team couldn’t be together in one physical location to strategize. “That was the unique challenge of managing this crisis, because we couldn’t all come together in a single setting—so we had to do it all virtually,” Bernazal says.

But with the help of the Everbridge platform, such coordination was possible. “In this case our collective security team and our professionals did a fantastic job in empowering folks to act on behalf of the company—to be nimble and to react and to make the best decisions they could at the time,” he adds.

The Visual Command Center was also used during the 2016 presidential coup d’état attempt in Turkey to help travelers reroute their journeys. A faction of the country’s armed forces organized and attempted to overthrow the government; more than 300 people were killed.

NOV had workers scheduled to travel through Istanbul, where military tanks were roaming the streets—there were even tanks rolling through the airport. “We have the travel itineraries of all our travelers in Visual Command Center, so at any given time, we can see all of our travelers in the world,” Dadd says. “Five travelers were going to be going through Istanbul very soon.”

Using a messaging feature in Visual Command Center to target specific travelers, security informed them they would need to change their travel plans and avoid Istanbul. “In a matter of literally minutes, we were able to push a message to our travelers through Visual Command Center to let them know what the situation was and to reroute their travel,” Dadd says. “So that’s how we find value in how we interact with our traveling workforce.”

FOR MORE INFORMATION: JEFF BENANTO, JEFF.BENANTO@EVERBRIDGE.COM, WWW.EVERBRIDGE.COM, 781.373.9879

FOR MORE INFORMATION: TSCM America (866.448.3138 www.tscmamerica.com)

• Corporate and Government Counterespionage Experts
• Nationwide Technical Surveillance Countermeasure Services (TSCM)
• Most Advanced Cutting-Edge Technology for Detection of Current and Emerging Eavesdropping Threats
• Technical Sweeps of Boardrooms, Conference Centers, C-Suites, Off-Site Meetings, Aircraft, and other Facilities
• World-Class Nationally Accredited Provider of TSCM Services
• Responsive, Efficient and Confidential (NDA)

EAVESDROPPING DETECTION SPECIALISTS
Nationwide Services 866.448.3138 www.tscmamerica.com

For product info #11 securitymgmt.hotims.com
The Privacy Problem

Private companies come together to demand that authorities create privacy regulations to protect users’ data and technology. By Megan Gates

Internet users generate more than 2.5 quintillion bytes of data every day and will create vast amounts more in the future as the Internet of Things (IoT) continues to grow, according to cloud-based operating system company Domo. There are benefits to the creation of this data—improved technology offerings, learning material for artificial intelligence programs, advances in medical science, and more. But there are also downsides if companies that collect this data are left unregulated, critics say.

One horrifying example came to light in the past two years when a Facebook propaganda campaign resulted in the emigration of more than 700,000 Rohingya who fled Myanmar to escape a campaign of ethnic cleansing targeting Muslims in the country. Thousands of others were killed.

The Facebook campaign was created by Myanmar military personnel, who coordinated over several years to spread false information—like allegations of rape and mass killings by Rohingya—across the Internet. The posts escaped Facebook’s notice, and human rights groups allege that they were used to incite murders, rapes, and the ultimate massive migration of Rohingya out of Myanmar to escape persecution.

Almost a year after Rohingya began fleeing Myanmar, Facebook—facing mounting criticism—hired the Business for Social Responsibility (BSR) to assess Facebook’s role in the violence in Myanmar.

The report found that Facebook was not doing enough to prevent its platform from being used to create division and incite offline violence. Facebook agreed with the report’s findings, and explained in a corporate statement by Alex Warofka, product policy manager, that it was making changes to the platform to prevent future atrocities.

“BSR provided several recommendations for our continued improvement across five key areas, in order to help mitigate the adverse human rights impact and maximize the opportunities for freedom of expression, digital literacy, and economic development,” Warofka wrote. “These areas include building on existing governance and accountability structures, improving enforcement of content policies, increasing engagement with local stakeholders, advocating for regulatory reform, and preparing for the future.”

Facebook is taking these actions independently because currently there is no regulatory framework that would require it to remove propaganda like that used by the Myanmar military.

This lack of legal guidance highlights a major problem in our current “data-industrial complex” that allows information to be “weaponized against us with military efficiency,” said Apple CEO Tim Cook in a recent speech at a European privacy conference.

“Platforms and algorithms that promised to improve our lives can actually magnify our worst human tendencies,” Cook explained.
“Rogue actors and even governments have taken advantage of user trust to deepen divisions, incite violence, and even undermine our shared sense of what is true and what is false. This crisis is real. It is not imagined, or exaggerated, or crazy.”

In his speech, Cook praised European lawmakers and California legislators who have enacted data protections for users (the General Data Protection Regulation and the California Consumer Privacy Act). But he said more needs to be done to protect users, so they continue to trust—and use—new technology.

“It is time for the rest of the world to follow [Europe’s] lead,” Cook said. “We at Apple are in full support of a comprehensive federal privacy law in the United States.”

Specifically, Cook articulated that this law would give users the right to have their personal data minimized, give users the right to know what data is collected on them, give users the right to access that data, and require that data be kept securely.

And Apple isn’t alone in its stance. Intel recently released a draft bill for the United States designed to optimize innovation and protect privacy.

“What the United States needs is a privacy law that parallels the country’s ethos of freedom, innovation, and entrepreneurship,” Intel said in a statement about the legislation. “That law needs to protect individuals and enable for the ethical use of data.”

Having a legal framework for data usage will help new technologies, such as artificial intelligence, solve global problems while creating economic growth, Intel added.

“We at Apple are in full support of a comprehensive federal privacy law in the United States.”

Intel’s suggestions are similar to Apple’s, including limiting the amount of data that is collected on users, requiring organizations to specify why they are collecting that data, limiting the use of that data, and requiring organizations to “adopt reasonable measures to protect personal data.”

Intel also explained that it recognized the need for a legal framework to prevent “harmful uses of technology and to preserve personal privacy so that all individuals embrace new,

IoT INNOVATION

A majority of companies polled in a recent study say they believe the Internet of Things (IoT) is critical to at least some of their business. Fewer are confident in their ability to control security, privacy, and data ethics as they adopt IoT technology.

Company perceptions on keeping pace with innovation

Say IoT is critical to business: 81%

Plan to invest in IoT security within the next year: 30%

Are very comfortable in building sufficient digital trust controls: 31%

SOURCE: The Journey to Digital Trust, PricewaterhouseCoopers, November 2018
data-driven technologies,” in the statement. “At Intel, we know that privacy is a fundamental human right and robust privacy protection is critical to allow individuals to trust technology and participate in society.”

Microsoft has also advocated for more robust regulation of the Internet and tech firms. In 2018, it worked with the French government to create the Paris Call for Trust and Security in Cyberspace, which was announced at the UNESCO Internet Governance Forum in November.

“The French government has worked to lay the foundation for the steps the world’s governments and other stakeholders need to take,” said Microsoft President Brad Smith in a Financial Times op-ed. “We should all hope that the other participants in Paris will participate in society.”

Privacy is a fundamental human right and robust privacy protection is critical to allow individuals to trust technology.

This is indicative of the reluctance of the United States on the national level to address privacy and cybersecurity regulations. This is unlikely to change in 2019 with U.S. President Trump in the White House and Republicans maintaining control of the U.S. Senate.

Varonis Tech Evangelist Brian Vecci says that private companies will lead efforts to standardize the regulatory field following actions by U.S. states—many of which have already adopted data breach disclosure laws and will likely consider legislation similar to California’s in the future.

“The big tech companies are very forward thinking,” Vecci says. “They tend not to think a quarter ahead or a year ahead, but five, 10, 20 years ahead—that’s the business they’re in.”

While in the past Americans may have assumed that a major data breach or cyberattack would press the U.S. Congress to act, Vecci adds that, following the Equifax breach, that’s unlikely to happen.

Instead, the push will come from private companies looking to ensure that revenues and trust in their products and services remain high.

“If no action is taken, we’re going to start to see a bit of a backlash,” Vecci says. “To maintain trust for their businesses to work, these firms are going to be at the forefront of putting that privacy regulation in.”

**ONE FALSE CLICK**

BY JERRY HUTCHESON. Published by Jerry Hutcheson; available from amazon.com; 190 pages; $18.95.

HELPING EXECUTIVES understand the challenges that cybersecurity poses is the goal of One False Click: How to Protect Your Company in the Coming Cyber War. The book explains cybersecurity from a business management perspective, instead of anchoring prevention in technology only. While technology is mentioned, the focus is on prevention using methodologies that can be found in risk management principles.

This is not a book about IT. It is a book about cybersecurity and how the business executive can understand the subject matter and apply prevention measures without having to be an IT expert. It is refreshing to see someone conceptualizing cybersecurity for what it is—a security issue rather than just an IT issue.

The author speaks in the language of executives, and there is no IT jargon. There are plenty of examples of risk management concepts from a business perspective such as return on investment, annual loss exposure, metrics, and results matrix. The author outlines the importance of leadership, roles and responsibilities, use of experts, security strategy, and policies and procedures. He underpins the prevention strategy in people and processes, these being the ingredients that are required to be successful in defending against the cybersecurity threat.

The book is well laid out. The first few chapters introduce us to cybersecurity, the current situation, where it is likely to go, the role of the security manager, and the four areas of cybersecurity. The rest of the book deals with security problem solving from a business management perspective and provides tools the executive can adopt while also drawing on the need for executives to become involved in preventing cybersecurity risks. The role and skills gap of CIOs and CISOs are also outlined.

This book will appeal to the business executive, business owners, general managers, and security managers. It will help them understand prevention from a business perspective while also providing them with the tools they need to oversee cybersecurity. IT professionals will value the book for its insight into how business executives think and what they need to know.

**REVIEWER: Dr. Declan Garrett is head of security unit at Louvre Abu Dhabi, visiting lecturer at Berlin Institute of Economics and Law, and a member of the ASIS Cultural Properties Council.**
dormakaba’s Exit Lane Breach Control technology employs real-time video analytics, system monitors and motion sensors that interface with airport systems to detect and identify suspect persons and objects left unattended. Plus, the modular stainless-steel construction allows multi-lane configuration to provide the highest throughput achievable. It’s time to replace the old guard with a new exit strategy that saves time and money – without compromising airport security or passenger safety. After all, security and savings are the key to a solid exit strategy.

dormakaba.us/ELBC-SM
Relationships

School resource officers are going above and beyond traditional law enforcement duties to build relationships with students, inspire educational growth, and prevent threats.

KEVIN WREN was working as a school resource officer (SRO) at a South Carolina high school in the early 2000s when he was called to the assistant principal’s office. Two female students were involved in an altercation about a boy—could the SRO help the girls mediate their way to a peaceful resolution?

But the violence only escalated when the two girls tried to talk it out. “We’re in the middle of the mediation, this girl flips out—next thing I know, she and I are both through the sheetrock wall in the assistant principal’s office,” Wren recalls of the incident. “So, we get up, we dust off…and I told her, ‘Jessica, you and I are going to become real close.’”

And become close they did. Jessica, who was also struggling in school, was initially resistant, but Wren began escorting her to every single class, every single school day.

“And from that day forward for about two weeks, I walked her every day to every one of her classes,” he says. “We built a relationship. It was great to watch her go from failing, and this huge issue over some boy—and she wound up graduating on time.”

Wren, who now serves as director of risk, security, and emergency management for Rock Hill School District in South Carolina, says he keeps a picture of Jessica on his desk to remind him of the impact SROs have on students’ lives.
“I’m not a former SRO, I’m a recovering SRO,” he quips. “Because once you’ve got it, and you’re there with the kids and you know it’s the right thing to do, you just miss that interaction.”

The role. SROs are involved in more than just law enforcement—experts say that role is a tertiary one compared to the education and relationship building that SROs participate in at schools across the United States, ultimately impacting the lives of students.

Recent events have highlighted the role of SROs, both for better and for worse. During the February 2018 Marjory Stoneman Douglas High School shootings in Parkland, Florida, in which 17 students and faculty were killed, a sheriff’s deputy working as an SRO was lambasted for remaining outside the school building during the shooting—rather than going inside and responding to the threat. On the flipside, an SRO at a high school in southern Maryland was praised for quickly intervening when a male student opened fire in the hallway, injuring two students in March 2018. Though it was the shooter who ended up taking his own life, the actions of the SRO were credited with eliminating the threat to those inside the school.

SROs are sworn law enforcement, in uniform and with a weapon, who are usually assigned to work in a school environment fulltime—though states as well as school districts across the United States have varying degrees of SRO involvement on their campuses. The SROs are assigned by their local police department and directly report to those agencies.

Some states are highly regulated when it comes to the role and involvement of the SRO—others rely heavily on local law enforcement bodies to assist when needed, but don’t necessarily have a fulltime officer interacting with the students and staff.

In New Jersey, former Governor Chris Christie mandated a legislative task force to draft guidance for law enforcement representatives in schools in 2015. “The recommendation was that there should be a school resource officer stationed in every school,” says Kevin Craig, school safety specialist at High Point Regional High School District who served on the task force.

Craig, a retired New Jersey police chief and member of the ASIS International School Safety and Security Council, says that while the recommendation is ideal in theory, there aren’t always enough resources to staff an SRO at each campus.

“Reasonably and realistically, implementing that, with costs and benefits and everything else, can become cumbersome for many police departments and schools, particularly because there are more than 600 school districts in the state of New Jersey,” he notes.

As a solution, the state came up with a new category of law enforcement officer—called a Class Three Special Law Enforcement Officer (SLEO)—in lieu of an SRO.

“Class three officers are retired police officers who have to go through the same school resource officer training that traditional SROs would have to go through,” Craig explains. “So, it gives [schools] a lower cost option to still facilitate that sworn law enforcement presence.”

Class three SLEOs must abide by several standards, including completion...
Reliability...When It Matters Most!

Two-way communications or one-way public address, GAI-TRONICS provides solutions to help you lead the way to a safer Campus.

of basic police training, retiring in good standing, and having been retired for less than three years.

So far, Craig notes that the class three program has been a success—adding that tragedies like Parkland and the shooting at a high school in Santa Fe, Texas, spurred schools to adopt the program.

“The first year of implementation they got off to a slow start, but many schools in New Jersey...are researching and implementing class threes in their schools,” he says.

NASRO. There is a national member organization for SROs, the National Association for School Resource Officers (NASRO), that provides standardized training for law enforcement working in schools.

Mo Canady, director at NASRO, says that working in an educational environment requires proper training.

“It’s the most unique assignment in law enforcement; there’s nothing else like it,” he tells Security Management.

“And you’ve got to be trained on how to properly work in that environment.”

NASRO recommends that SROs have at least three years of experience in law enforcement before being assigned to a school.

“At one minute, they have to be teaching a group of kids in a classroom or mentoring a student, and at the flip of a switch—in a split second— turn into the best tactical officer the department has to be able to stop a violent incident,” he says. “So, it’s quite a balance we’re talking about.”

**Guidance on Threat Assessment Teams**

*By Cody Mulla, CPP*

Recent guidance from the U.S. Secret Service, Enhancing School Safety Using a Threat Assessment Model: An Operational Guide for Preventing Targeted School Violence, offers baseline information for developing a threat assessment team (TAT) to mitigate potentially violent or devastating events at K-12 schools in the United States. The Secret Service advocates for a five-step process to establish a TAT with a multidisciplinary approach to information sharing. For each step, the author will provide guidance that extends beyond the scope of the Secret Service report with additional threat prevention measures.

1. Establish a multidisciplinary team. The TAT is designed to direct, manage, and document threat assessment processes. Assemble a team from a variety of disciplines, which may include teachers, school guidance counselors, coaches, school resource officers, mental health professionals, and school administrators. Have a designated leader with the authority to act immediately in cases where time is of the essence. Meet on a regular basis and when needed if there is an emergent concern. These meetings should include dealing with potential threat indicators, training and role-playing focused on building confidence and capability, and building rapport and confidence in other team members.

   **Additional guidance:** Threat assessment is an intelligence-led activity and requires a certain skill set to synthesize information. Schools could partner with an agency or consider employing an employee with an intelligence background. The Multi-State Information Sharing and Analysis Center (MS-ISAC) also offers valuable trend information on physical and cyber threats that could be useful for the TAT.

2. Define prohibited and concerning behavior. Concerning behavior progresses through a continuum, and policies must consider warning signs, which include “a marked decline in performance; increased absenteeism; withdrawal or isolation; sudden or dramatic changes in behavior or appearance; drug or alcohol use; and erratic, depressive, and other emotional or mental health symptoms,” according to the report. Policies and procedures should be set in place to monitor and direct action to collect additional information to consider if these are indeed a concern.

   **Additional guidance:** The Secret Service does allude to a continuum, but there is no specific guidance on how to categorize threats. A more in-depth understanding of transient and substantive threats...
is needed. It may be advisable to develop a tailored process map for each TAT, which describes each step and indicates responsibility in each phase to avoid anything falling through the cracks.

3. Create a central reporting system. Establishing a central reporting system is crucial to all other threat assessment activities. Schools should establish multiple streams of information that could include online reporting, email, phone, and face-to-face communication. No reporting should be dissuaded but educating the school community on what to report will increase the validity of information. Document thoroughly when responding to each report, categorizing threats, and determining whether to act. Anonymous reporting should be an option for those who are uncomfortable coming forward in a formal or public way. It is important to handle each case with professionalism, considering privacy and confidentiality concerns.

Additional guidance: Consider partnering with an Information Sharing and Analysis Center (ISAC), which is a nonprofit organization that provides an avenue for two-way sharing between the public and private sectors. Though ISACs have traditionally dealt with cyber and physical security, the model could be used to develop information sharing practices related to threat assessment.

4. Determining the threshold for law enforcement intervention. Law enforcement intervention may be needed in some cases, though it may not be involved in all threat assessment efforts. Create policies and procedures to indicate when law enforcement should be involved—for example, in cases that deal with weapons, threats of violence, and physical violence. Law enforcement should be involved when elements of a crime are present.

Additional guidance: Certain privacy laws set limitations on law enforcement activity when it comes to minors. School administrators and the TAT should familiarize themselves with state law before developing policies and procedures around law enforcement response.

5. Establish assessment procedures. Establishing threat assessment procedures will help paint an accurate picture of the student's thinking and behavior, formalize a reporting structure, and identify appropriate interventions. Documentation is once again stressed, with creation of forms and templates to capture necessary information. The report recommends a community-wide approach and encourages a brainstorming exercise on sources of potentially helpful information. This exercise can be repeated once an individual of concern is identified for information more specific to that person. Additionally, social media should be examined to gain information, interviews should be conducted, and the student's locker should be searched.

Additional guidance: The Secret Service guidance seems to only consider internal threats—mainly students—but narrowing the focus is a risk in and of itself. A threat could be anyone: a teacher, contractor, administrator, or someone not associated with the school. Threat assessment is a necessary part of threat prevention at every K-12 school. Threat assessment programs and teams will be more successful if they are a function of an overarching enterprise risk management process, fueled by both internal and external sources of information.

CODY MULLA, CPP, HAS 20 YEARS OF EXPERIENCE IN SECURITY AND CRISIS MANAGEMENT. HE HAS WORKED SUPPORTING BOTH THE PRIVATE AND PUBLIC SECTORS AND IS A MEMBER OF THE ASIS INTERNATIONAL SCHOOL SAFETY AND SECURITY COUNCIL AND THE UTILITIES SECURITY COUNCIL.

Go to SM Online to read the Secret Service guidance on threat assessment teams.
MITIGATE THREATS BEFORE THEY EMERGE
THE WORLD HAS BECOME INCREASINGLY VOLATILE, CREATING A DISRUPTIVE ENVIRONMENT FOR BUSINESSES.

Faced with growing threats, from natural disasters to human conflict, corporate security and business resilience teams are being tasked with managing a greater number of ever-changing risks that occur at greater frequency but in even less time. A Fortune 100 director who oversees corporate security and risk management quickly realized that the institution’s old processes and systems had simply become obsolete, leaving the organization at risk.

Despite increasing investments in security solutions, the director found that his organization had prioritized the acquisition of physical security systems, from access control to closed circuit television (CCTV), without considering how these systems would integrate with one another. “It was extremely frustrating knowing that we owned all this data but that we couldn’t access it. Our systems were disconnected, or they required us to manually extract and repackage the data. Our analysts were using Excel and pivot tables, trying to extrapolate critical data, and in the end, the results were hidden in cumbersome reports,” said the director. “This approach wasn’t in real time, and given the severity of threats we face every day and the size of our organization, it was imperative to find a solution for the health of our business.”

When evaluating solutions, the director needed to find an application that would not only provide his team with real-time access to mission-critical data but would also integrate with his organization’s existing security investments. “We have so many disparate data streams from access controls, consumer data, crime feeds, [and] terrorist threats, but we also have staff at our thousands of branch locations that could offer us valuable information.”

Like most corporate security executives, the director needed one holistic view of the institution’s organizational data to extract actionable insights. “Implementing Esri’s corporate security solutions allowed us to connect all of our existing technologies and staff. For the first time, we were able to capture and instantly upload incident data from the field. We no longer rely on spreadsheets and emails, and our analysts are able to identify potential threats before they happen.”

Scenarios like these are common in today’s corporate environment. As businesses continue to grow in new and existing markets, they have inevitably become exposed to a greater variety of risks. Unfortunately, many investments in security solutions only address a narrow subset of these risks and do not integrate well together. Through utilizing Esri’s location intelligence solutions, corporate security and risk teams can leverage all their data and unleash the full potential of their existing investments. By providing a common framework for data integration, analysis, and cross-departmental reporting, Esri’s solution equips executives with the tools needed for decision-making before, during, and after a crisis.

To learn how location intelligence can empower your corporate security and business resilience teams to mitigate threats, visit esri.com/ASIS.
According to Canady, training in special education and diversity are critical. “If you hear someone talking about ADHD, or a manifestation of a student’s disability, it can be very frustrating as an officer to come into that environment and not understand some of those things that are being talked about,” he says.

**Responsibilities.** The shadow of an active assailant threat looms large over U.S. K-12 schools, and SROs are being prepared to protect their campuses should the event arise. Still, Canady says SROs must remain focused on the day-to-day threats that are much more likely to occur and affect student safety.

“Most SROs, most schools are never going to face an active shooter event,” Canady notes. “It’s a high impact event with low probability, and so we have to be prepared for it.”

He says the higher likelihood on any given day for an SRO is dealing with students who may have problems at home, abuse narcotics, or are involved in criminal mischief.

“This is where we want SROs to be actively engaging with students in a positive way, through informal counseling and through education,” Canady says.

Still, SRO training would be remiss not to include active assailant response tactics. “Back in the Columbine days, we were waiting for SWAT teams to arrive,” Craig notes of SROs. “Now the expectation is that the first officer on the scene is going to enter the building and try to neutralize any threat and any active shooter incident.”

When it comes to day-to-day classroom management, Craig says SROs should not cross the line between basic disciplinary tactics and using excessive amounts of force against a student who misbehaves.

“We’ve seen some difficult situations throughout the country where force has been used, sometimes excessively,” he notes.

While those difficult situations may be rare, some have garnered national attention. A viral video, for example, surfaced from a South Carolina high school in October 2015. It depicted an SRO slamming a student to the ground after she refused to leave class for causing a disruption. The video called into question whether SROs should be as involved in classroom disciplinary issues.

Craig iterates that if a student refuses to put his or her cellphone away, for example, that’s the type of discipline a teacher, administrator, or even school security staff should handle, not the SRO.

“If the behavior rises to the level where someone’s being physically assaulted—there’s a physical danger of physical threat to that student or to someone else—those are the situations where SROs are going to get involved,” he notes.

**Relationship building.** Experts emphasize that one of the most important functions of SROs is their ability to detect and prevent threats through relationships with students.

“There are multiple situations where a good SRO...has come to discover that we have a child that’s in danger—in a situation at home or wherever it may be—and they have taken steps to get the child help,” Canady notes.

He recalls the case of a veteran SRO in the southeast United States, who was called to a classroom to deal with a disruptive female student.

“She walked her down to the administrative offices...and just sat down and talked with the student,” he says. “And what came to light in this discussion is that she was being sexually abused by her mother’s live-in boyfriend, and it had been going on for over a year.”

In that case, the SRO was able to help make a case against the mother’s abusive boyfriend, and he was sentenced to jail.

“So instead of having a situation where we’ve got a student arrested for disorderly conduct, we had a very good SRO in place that knew there was something more to the story, and took the time to deal with it,” Canady says. “SROs are doing that all over the country right now.”

---

**We’ve seen some difficult situations throughout the country where force has been used, sometimes excessively.**

Tips given to SROs by students or even members of the community also prove invaluable in stopping threats or determining their credibility. Craig notes that social media has become a breeding ground for information on possible threats to student safety.

“Our students, they are on social media all the time, so they see a lot more and hear a lot more of potential threats and things that could potentially impact the school district than the adults,” he says.

In one instance, a student posted a threat on social media that centered around a school football game. After the SRO was notified of the post, the school identified the student and conducted a risk assessment, ultimately concluding that the threat was not a credible one.

“Our students are very comfortable with the fact that they can communicate with our SROs and let them know about those threats...so they can try and take preventative action, rather than have to react after something happens,” Craig explains.

**Partnerships.** Partnering with other stakeholders is key to an SRO’s success. Wren notes that it’s critical to bring the officers and administrators together, as well as the three law enforcement agencies in his school district, to conduct training, drills, and tabletop exercises.

“We bring our SROs and administrators together every year for a training session, and we talk about emergency planning, emergency management,” he says. “We talk about security, we reiterate our policies, and our memorandum of agreement between the agencies.”

NASRO continues to be involved in initiatives and partnerships across the U.S. K-12 schools, and SROs are going to get involved,“ he notes.
country to help improve the training and overall effectiveness of SROs. Former U.S. Attorney General Jeff Sessions spoke at the organization’s national conference in June 2018, where he announced $25 million in funding for training and technology to improve school emergency reporting.

“I believe this funding is going to make you more effective—and that will make the children of this country safer,” Sessions said.

In July, Canady had the opportunity to testify before the Federal Commission on School Safety at the White House, along with two other NASRO board members. He says he believes the future of the organization partly depends on this public-private collaboration.

“We’ve been engaged on a lot of things over the last few months...so that’s exciting,” he notes. “We have a great relationship with the federal government right now.”

In addition, the organization recently released new standards on school-based policing that were added to the Library of Congress.

While stopping threats, providing guidance, and attempting to change students’ lives for the better are the goals for an SRO program, Wren emphasizes that it’s the student who must be willing to make a change in his or her own life. Another photo on his desk, opposite of Jessica’s, serves as a stark reminder of this truth.

As a soccer coach during his SRO days, Wren had a player named Mike who was hard working and dedicated. But over time, he began skipping practice, and Wren did his best to inspire the boy to change. Eventually, Mike went down a bad path, which the adults in his life were ultimately powerless to stop.

“He was arrested with another kid and eight other football players for armed robbery, and he just got out of prison this past year,” Wren says. “It’s still up to the student to make the right decision...I know that I did everything I could do.”

He adds, “SROs...they are going home with a clear conscience that they have done everything they can either to prevent something from happening, or to build that relationship with that student to get them through to graduation.”

HOLLY STOWELL IS FORMER ASSOCIATE EDITOR AT SECURITY MANAGEMENT.
Serving the New Generation

ASIS President Christina Duffey, CPP, shares her thoughts on building a security career, connecting through ASIS, and investing in the future of the profession.

How did your career begin? What drew you to the security industry? A. The journey began shortly after I left the Canadian Armed Forces, a Reserve Communication Squadron. At first, I wasn’t sure whether a transitional job as a security officer would lead to the next big thing—a career, in who-knows-what, because security really was not considered a profession yet. However, it was not long before I sensed that there were opportunities well beyond my security officer role. Back then, technology was just starting to slowly creep into the physical security realm. I knew that gaining experience in roles that utilized “the computer” would be key to building valuable skills for the future. But the ‘90s were in no way a straight career path and stacked with plenty of obstacles, gender being one of them. Over time, as the opportunities got bigger, so did the risk of failing.

What were some key lessons you learned early in your career? A. The blueprints laid out by my supervisors were a great first step, but soon true identities emerged. It was not long before I realized that increasing vocational knowledge and obtaining industry certifications was critical, but watching supervisors and mentors was where the real lessons were learned. I studied each leader’s history, who they were, how they got there, and the impact they were making on people, programs, and the community. By doing this, I learned both the good and the bad; watched and learned from the risks taken and how to recover; and discerned how arrogance and a lack of values can erode integrity and a personal brand.

What do you see as the current opportunities for security and those who serve in the industry? A. It is not about living in the past; the real opportunity is for leaders to leverage their experience and insights to encourage the future. For example, we must convey the importance of picking mentors and leaders. They challenge but educate with kindness to inspire through the difficult times. Mentors who are also direct supervisors have a vested interest in individual success because it helps their success. But this relationship may be limited to the immediate work environment, which underscores the importance of volunteering and serving the security industry. Expanding your network to include leaders who are willing to pass along knowledge with no personal gain will elevate you to the next level. At some point, it shifts from listening to the stories to telling your own story. This is when serving the new generation truly happens and it becomes about selflessly helping others gain wisdom and resiliency.

How can ASIS be an asset in the security industry? A. Through industry networking and relationships, you will expand your connection to expertise, resources, and opportunities. ASIS International provides an excellent path to engage with leaders outside the traditional work circle to build technical knowledge. Expanding your network to include leaders who are willing to pass along knowledge with no personal gain will elevate you to the next level. At some point, it shifts from listening to the stories to telling your own story. This is when serving the new generation truly happens and it becomes about selflessly helping others gain wisdom and resiliency.

How can ASIS serve emerging security professionals where they are? A. Serving the new generation is not an easy task. Solely pulling from our past and the trenches we grew up in does not provide the necessary road map for emerging leaders. The new generation is smart, educated, healthy, and technologically strong. They want to get there faster and better. “Old school” approaches should not hold them back, but rather equip them with experience that embraces their new ideas and ways.

It is not so much what you teach, but how you teach it. Passing wisdom that is meaningful, inspirational, ensures vocational skill development, and educates for the unknowns is critical. But most importantly, the best mentors lead by example. Go beyond sharing wisdom, model the traits and behaviors emerging leaders should embrace. Our duty is to carry the new generation by helping to maintain a balance between technology—with its speed and immediacy—and natural unfolding of knowledge and wisdom gained over time.
A world of vital security news delivered to your inbox.

Security Management Daily
is an exclusive e-newsletter for ASIS members. It offers the top 10 security headlines and is e-mailed daily.

Security Management Weekly
is a free e-newsletter for anyone who would like to subscribe. Receive the week’s 15 security headlines.

Check out the Security Management newsletters’ new features and design. To subscribe or resubscribe, e-mail ASIS International: asis@asisonline.org.
TRAVEL SAFETY | BY LILLY CHAPA

PHOTOS BY ISTOCK
What should providing true duty of care to employees actually look like?
That’s the question that Shelby LeMaire, global travel manager at iRobot Corporation, asked herself almost a decade ago when she was tasked with consolidating the organization’s global travel program. The company, which sells technology ranging from Roomba vacuums to military-grade robots, has offices in 15 countries and often sends employees into war-torn areas to provide support to the military.

When LeMaire began researching travel programs, she realized she wanted to do more than just track employees as they moved around the globe—she wanted to prepare them for the risks they might face. “As I started to do some research about that, I realized there was this obligation called duty of care, and that’s what this fell into,” LeMaire says. “At that time, there really wasn’t a lot of literature...so I did a significant amount of research on my own and I realized that we needed to fulfill this duty of care obligation. My first reason for wanting to put the program in place was for employee safety, but then I realized as a company we have a responsibility to our travelers.”

LeMaire presented her argument to iRobot’s executive team, where she cited legislation and case law, as well as educating them on the concept of duty of care because they were unfamiliar with the term. When the organization approved an expansion of its travel management strategy, LeMaire partnered with International SOS, a medical and travel security firm, for organizational support.

“Our program has evolved over time, but I look at duty of care differently than a lot of people,” LeMaire notes. “Some people feel that they give their employees a card that has a number to call, and I say that’s not fulfilling duty of care responsibilities.”

Having International SOS handle the risk intelligence, employee tracking, and medical response aspects of employee travel was a huge help, but LeMaire went on to augment traveler preparedness with a predeployment education plan for iRobot employees, which included educating them on travel best practices and risks specific to the area in which they were traveling. “That was important to me because I realized that not only do you need to have a response plan...
TRAVEL SAFETY

Travel Best Practices

Matthew Porcelli, CPP, security manager and consultant, sat down with Security Management to discuss ways to stay safe during travel, for those monitoring traveling employees and those traveling alike.

Be alert, especially at the airport.
Airports are prime spots for bad actors to target unwitting travelers. Staying alert and under the radar is key, Porcelli says. He gives an example of a woman who was abducted by three people after getting off a plane in Thailand—even though she was surrounded by other passengers.

“I saw the CCTV footage, and nobody even picked their heads up and looked,” he says. “Do not have tunnel vision.”

This is especially important because aggressors are constantly monitoring their surroundings looking for victims—and the best defense is to be just as vigilant.

“Aggressors will people watch,” he notes. “They are not dummies. They will know who to target and will do their research just like a security professional will.”

Keep your documents safe.
Travel document retention and security is especially important while traveling abroad, because losing such objects not only makes it difficult to fly back home but puts sensitive information in the wrong hands.

“Don’t bring your passport out with you—make a copy of it to take out with you, keep the original locked in the hotel safe, and also keep copies at home and with your office coordinator,” Porcelli says.

He also recommends not leaving a business card or contact information in the plastic windows on luggage—that’s a good way to become a target.

Do your own research—and make liaisons abroad.
Even if an organization uses a travel and risk management company, it doesn’t hurt to stay up-to-date on current events in upcoming destinations. The Overseas Secular Advisory Council (OSAC) and the U.S. State Department also provide resources for travelers. Porcelli suggests networking with other professionals in potential travel destinations—that way you can check in with them about the climate of the region before you arrive. Additionally, using tools such as Google Earth ahead of a trip can help plan routes and quick exits if needed.

if somebody needs medical or security assistance, but from a company and an employee perspective you want them to have a successful mission and you want them to be prepared, not only for the risks that they are facing but other things such as IT equipment, currency, and how to avoid the risks that you’re going to face as you’re traveling overseas,” she explains.

Predeparture activities are also based on a risk grading that International SOS provides to the organization. “If there’s a risk grading that’s higher than a certain grade, then that’s escalated to the executive level where I manage that process,” LeMaire explains. “From there we have specific requirements for those travelers that are going to high [risk] and extreme destinations where we do one-on-one briefings with them to prepare them.”

While the training and risk analyses may cover worst-case scenarios, LeMaire says it’s not meant to scare employees—it’s to make them understand what processes and tools are in place if they do encounter a problem.

“It’s really important that the travelers have that comfort level knowing that when they are abroad, they have tools that can help them navigate through situations,” she explains. “I can just imagine companies that don’t have these programs in place, how an employee would feel—I would feel terrified myself if I were overseas not knowing what to do if I suddenly became ill or had an accident of any sort.”

It’s clear that LeMaire is passionate about developing an extensive travel program for iRobot. She acknowledges that many organizations may not build out such a robust program because they only consider large-scale crises that rarely take place. But she says the program goes beyond terror attacks or natural disasters—it’s especially helpful if an employee falls ill abroad.

“It’s not just the high-risk situations that people think of—we promote the usage of International SOS for any and all concerns while you’re traveling,” LeMaire explains. “One of the things that people think of when they hear about risk abroad is something like the Paris attacks. I think a lot of companies think, ‘Oh, it’s not going to happen to us,’ but
the vast majority of cases that any company is going to encounter are medical cases. We’ve encountered many medical situations as people have traveled abroad, and one of the key things is that you want to be able to respond to them in a timely matter.”

Because of this, when LeMaire worked with the organization’s executive team to create an emergency response plan of core activities they would carry out from the office, she also kept in mind that not all travel issues would be severe. She created a communications policy that only alerts executive-level team members if the problem is severe enough, which then triggers the response plan.

“There are things that we as a company need to put in place that were consistent among the security issues, the medical issues, so this just helped us stay focused and not panic” if something did happen to employees.

More recently, iRobot has expanded its travel program to apply to employees traveling within the United States, as well.

“We need to also assume responsibility and liability of our travelers traveling domestically,” LeMaire says. “It may not be as robust of a training, but we need to make sure that we’re capturing all of our travelers regardless of whether they are traveling in their home country or abroad—that we’re providing that same level of care we do for our international employees.”

During LeMaire’s research into the importance of duty of care for an organization, she learned she cannot discount the role liability plays in well-rounded travel programs.

“When it comes to the liability perspective, that is not what drove my company to put the program in place,” she says. “But when you have an incident and you are faced with a claim, it’s important as a company that you can prove that you conducted predeployment training.”

LeMaire acknowledges that building iRobot’s travel security program has been a long process filled with a lot of research and legwork, but that it’s paid off. For other companies looking to build or expand their travel policies, she recommends they partner with a firm that can provide risk assessments. LeMaire also recommends augmenting that with in-house training and policies.

“All of our employees are thoroughly trained so that they are well aware of what our vision and strategy is in this company of promoting safe travel,” LeMaire says. 

LILLY CHAPA IS A FORMER ASSOCIATE EDITOR WITH SECURITY MANAGEMENT.
One after another, reports involving allegations of sexual misconduct continue to be made public. Many of these reports follow a similar scenario—a middle-aged, executive-level man allegedly uses his power and influence to target, and sometimes sexually assault, a person over whom he has power. When true, the events behind these stories can leave the victims and their families scarred and damaged for life. Given what’s at stake, many victims and their advocates have turned to Twitter to express solidarity and expose their alleged abusers, using the #MeToo hashtag. By now, the #MeToo movement has become a worldwide phenomenon, and its impact has put employers of every stripe on notice.

In the United States, the federal government’s Equal Employment Opportunity Commission (EEOC) has been vocal on the topic. Recently, EEOC Commissioner Chai Feldblum publicly offered three overarching recommendations to employers attending an Ogletree Deakins Workplace Strategies conference: Change workplace culture; hold people accountable;
FROM CONSENSUAL TO CONCERNING

Investigations in sexual harassment must address a variety of situations, many of which do not fit the typical #MeToo mold. For example, in one real-life incident, a romantic relationship turned sour, requiring security to launch an investigation.

The participants, whom we will call Christopher and Meredith, met each other at work. He was a regional vice president and she an entry-level analyst. Over a period of several months they began to date, and then entered into a consensual romantic relationship. Christopher started acting jealous and possessive, insisting that he know with whom Meredith talked, exchanged emails, and took breaks while at work. Meredith later described this as romantic obsessive behavior. She decided to terminate the relationship.

Christopher, still driven by possessive feelings, began to stalk her. He started following her home after she left work. Meredith no longer felt safe at work or anywhere else, and she reported her concerns to HR. Pursuant to established protocols, HR immediately reached out to the director of corporate security and requested assistance to investigate Meredith’s allegations. Security, working with the legal department, determined that the matter was sufficiently work-related and that, if true, the claims were actionable. Thus, two investigators were assigned. The security director and HR discussed and defined the investigation’s objectives.

Meredith submitted to a formal interview. She revealed that not only was Christopher constantly monitoring her at work, but he was following her everywhere, even when she was on vacation. Further investigation produced evidence that Christopher used the organization’s email system to communicate threats. In addition, Christopher was using company computers to store inappropriate images of Meredith, which were secretly taken by him without her consent.

Though engaged by HR, the investigation team reported to general counsel, thus preserving the attorney work product privilege. Upon viewing Meredith’s written allegations, Christopher’s threatening email messages to her, and the stored images, counsel advised HR that Christopher’s termination was both appropriate and legally defensible. However, counsel also recommended that Christopher be interviewed and asked to explain his behavior and provide any extenuating circumstances or mitigating evidence.

During the subsequent interview with the investigator and his witness, Christopher conceded his obsession with Meredith and his related behavior. In writing, he agreed to cease this unwanted behavior, resign, and never communicate with Meredith again.

Following the acceptance of his resignation, Christopher left quietly. This case reveals a few valuable lessons. One is that a team approach to #MeToo investigations improves efficiency and results. HR, security, and general counsel all worked together, and had important roles to play. Another is that allowing the terminated employee to leave with his or her dignity intact usually costs nothing and often produces priceless results.

and implement the right policies, procedures, and training.

These directives are helpful, but seasoned security professionals, like their counterparts in HR, know that the problem requires more than recommendations and policy tweaks. Experienced security managers know that workplace behavior is modified and office cultures are changed when allegations of misconduct are taken seriously and investigated properly and thoroughly. Together, these serious attitudes and activities buttress what ethics and compliance experts call an organization’s compliance regime. When that regime is fair, disciplined, and combined with sound policies, clear expectations, and exemplary leadership, it forms the foundation of the organization’s culture and, ultimately, its reputation and identity.

Recognizing this, organizations of all sizes are increasingly turning to security professionals to either assist HR in conducting internal investigations or to conduct the investigations themselves. This is a serious responsibility, so it is important to keep in mind that a successful workplace investigation is a complex undertaking. It is time consuming and fraught with the potential for legal liability. It can also be expensive.

A proper investigation requires an intricate mixture of skill, experience, and patience. Those who attempt one without an understanding of the fundamentals are more likely to fail. The case study (at left) is provided to help the reader better understand how these fundamentals play out during an investigation.

**Fact Finding**

Experienced investigators know that few workplace activities invoke so much risk—and at the same time, so much opportunity—as an investigation. An improperly conducted workplace investigation can be ruinous and harm the careers of everyone involved. But a well-executed investigation bolsters an organization’s culture, which in turn enhances its reputation and its identity.
The processes used by successful investigations usually have similar attributes.

Successful investigations often rely on teams. In #MeToo investigations, the typical team includes three groups: fact finders, advisors, and decision makers. Fact finders gather information. They take direction from the appointed advisors and pursue the investigation’s objectives by means of thoughtful and deliberate fact-finding. Their purpose requires them to be objective, so they must do their work in a fair, impartial, thorough, and purposeful manner.

Fact finders’ tasks often include the gathering and proper preservation of physical, electronic, and testimonial evidence. Their results are typically packaged in a formal report and ultimately provided to the decision maker by way of the advisor. Under ideal circumstances, that advisor is legal counsel, so the fact finder’s report can be designated as attorney work product and shielded against unwanted discovery or disclosure. This practice is not nefarious; it is legal and proper and often in the best interest of all parties.

Process

To fulfill the objectives of the assigned investigation, the effective fact finder must have a process. Remarkably, many fact finders and decision makers, regardless of their level of experience or training, have little or no process to work with. Lacking this, the fact finders often spend more time and resources on their tasks than necessary, produce inconsistent results, and create unnecessary liabilities for those they serve. No investigation, regardless of its objectives or scope, can be successful if not properly engineered and driven by process.

Although certain details may differ from incident to incident, the processes used by successful investigations usually have similar attributes. The investigation has meaningful and well-defined objectives; it is properly and lawfully executed; it is fair and impartial; and it produces results that are accurately documented and communicated.

Also, to achieve maximum efficiency, an investigation should unfold incrementally and progressively, in distinct phases. Each phase should be engineered to build on the phase that preceded it. Generally, #MeToo investigations include these phases: assessment; preparation and planning; information and evidence gathering (fact finding), which usually includes the interviewing of the complainant; and verification and analysis, which invariably includes the interviewing of the alleged wrongdoer.

The investigation process should also be open to the possibility that additional complainants may come forward, necessitating the expansion of the initial investigation. Indeed, organizations that are experienced in investigations often anticipate both new and expanded allegations once the investigation of the initial complaint begins. This anticipation helps the organization craft and implement containment strategies and bake them into the overall investigative approach.

For example, one such containment strategy is to lock down the scope of the initial allegations with written statements provided by the accuser. Doing so prevents subsequent embellishment of the initial complaints.

As the investigation progresses, some fact finders put all their focus on the third phase—information gathering and the interviewing of the accuser—and then once they have amassed a rich collection of facts, evidence, and information, they conclude their investigation. This is a mistake, because...
even the most impressive collection of evidence requires analysis and verification. Without clarifying analysis, those to whom the fact finders report may receive an incomplete result, which may deny them a thorough understanding of the matter.

The four phases of the investigatory process give the fact finder the structure necessary to be effective. They also help when it comes to optics; following a phased process helps the fact finder transcend the dated image of a bumbling corporate gumshoe and may elevate him or her to the professional standing of an expert investigator.

Results and Metrics
Fact finders should never play the role of decision maker. To do so is unfair and creates the appearance of prejudice. Sadly, HR professionals make this mistake frequently.

In many organizations, HR is routinely responsible for all internal investigations. In addition, HR either decides the appropriate discipline or makes recommendations regarding such to the decision makers. The criminal justice equivalent of this would be for law enforcement personnel to determine the punishment of those they arrest—clearly, not a wise practice. Similarly, investigative best practices call for all final decision making, as well as the disbursement of even the most impressive collection of evidence requires analysis and verification. Without clarifying analysis, those to whom the fact finders report may receive an incomplete result, which may deny them a thorough understanding of the matter.

The four phases of the investigatory process give the fact finder the structure necessary to be effective. They also help when it comes to optics; following a phased process helps the fact finder transcend the dated image of a bumbling corporate gumshoe and may elevate him or her to the professional standing of an expert investigator.

Results and Metrics
Fact finders should never play the role of decision maker. To do so is unfair and creates the appearance of prejudice. Sadly, HR professionals make this mistake frequently.

In many organizations, HR is routinely responsible for all internal investigations. In addition, HR either decides the appropriate discipline or makes recommendations regarding such to the decision makers. The criminal justice equivalent of this would be for law enforcement personnel to determine the punishment of those they arrest—clearly, not a wise practice. Similarly, investigative best practices call for all final decision making, as well as the disbursement of disciplinary or corrective action, to be a separate process from fact finding, and not conducted by the same people.

Like most effective processes, the investigatory process should generate measurable results. Frequently, organization leaders will measure results in terms of the actionable evidence accumulated. However, the first and most immediate metric should be return on investment (ROI). For example, properly engineered and executed investigations generally produce tangible, measurable results such as the recovery of stolen property or money, the termination of dishonest employees or vendors, or successful prosecution. Other possible measurable results are civil recovery, restitution, damage awards, and successful insurance claims.

However, when investigating a #MeToo allegation, the achievement and recognition of measurable ROI is more difficult. Still, process-driven investigations enable the ability to generate statistical results that can be used over time to measure effectiveness and identify opportunities for process improvement. The ASIS International Investigations Standard (ANSI/ASIS INV.1:2015) identifies this methodology as the Plan-Do-Check-Act (PDCA) model.

When properly used, PDCA provides a repeatable and scalable framework for the conduct of one’s #MeToo investigations. Without process and structure, the investigator has no means
to measure results and show value to their customer. Even worse, the process becomes more vulnerable to claims of bias, ineptitude, and discrimination.

**Legal Issues**

Workplace investigations are fraught with liability. Internal investigations, by definition, involve the investigation of people who have a relationship with the organization. Usually, they are people the organization employs or does business with. Many consider themselves “insiders.” As such, they have special rights and expectations. They may carry a sense of entitlement and self-importance.

These considerations add to the complexity of the fact-finding process, and to the reaction of the subject to the investigation’s findings and management’s corrective actions.

**The first and most immediate metric should be return on investment.**

Clearly, this path is filled with legal obstacles and challenges. On the other hand, the totality of these complexities gives the properly prepared and equipped employer a decisive competitive advantage. The #MeToo investigator should have at least a working knowledge of criminal, civil, and employment law. The employer that can efficiently bring an end to workplace harassment, discrimination, or a toxic workplace without litigation or a public relations debacle has a significant competitive advantage over the employer that cannot. Thus, a skilled and savvy investigator can be an asset to almost any organization.

---

**EUGENE F. FERRARO, CPP, PCI, CFE**

(Certified Fraud Examiner), SPHR (Senior Professional in Human Resources), is Chief Executive of ForensicPathways, Inc. He is a former member of the ASIS Standards and Guidelines Commission and has been a member of ASIS International since 1987.
Her predecessor, Richard E. Chase, CPP, PCI, PSP, serves as chairman of the board in 2019, while 2018 Treasurer Godfried Hendriks, CPP, succeeds Duffey as president-elect, and 2018 Secretary John A. Petruzzi, Jr., CPP, takes on the role of treasurer.

Malcolm C. Smith, CPP, head of risk management for the Qatar Museums Authority, joins the Board Management Committee as secretary in 2019. Smith is a South African citizen with more than 30 years’ international working experience in security and risk management. He has held several senior management roles in the public and private sectors, including head of global security at Sasol; group head of security and safety services at Nedbank; and commissioned officer in the South African Defense Force.

AS THE CALENDAR FLIPS TO 2019, the members of the ASIS International Board Management Committee assume new roles for the new year.

Christina Duffey, CPP, senior vice president and Midwest regional director for SOS Security, is president of ASIS International. With more than 25 years of experience in contract security management in the United States and Canada, she has extensive knowledge and experience in asset protection. She served as 2011 president of the ASIS Professional Certification Board and has been a member of the ASIS Board of Directors since 2014.

NEW BOARD MANAGEMENT COMMITTEE

ASIS EDUCATION 2019

From creating a new website to launching the innovative ASIS Connects platform, ASIS showed a clear commitment to enhanced technology in 2018. The Society continues to transform engagement with the security profession via forward-thinking, engaging education platforms and programs.

The ASIS Learning Exchange—launched in late 2018 at learning.asisonline.org—gives a fresh look and improved searchability to online learning programs. Learning Exchange is a one-stop shop for ASIS online education offerings, including online courses, webinars, and GSX education recordings. Programs are organized by topic, content type, and career level. Users can browse and purchase individual programs or view on-demand recordings with their webinar subscription.
For those who prefer to attend educational sessions in person, here is a full schedule of 2019 classroom programming:

**25–28 February**  
Savannah, Georgia, USA  
- CPP/PSP Review  
- ASIS Assets Protection Course: Principles of Security (APC I)

**24–26 June**  
Atlanta, Georgia, USA  
- Risk, Threat, and Vulnerability Assessment  
- Enterprise Security Risk Management  
- Executive Protection  
- ASIS Assets Protection Course: Practical Applications (APC II)

**8–9 September**  
Chicago, Illinois, USA  
- CPP/PCI/PSP Review

**4–7 November**  
Seattle, Washington, USA  
- Crisis Management  
- Violence Assessment and Intervention  
- Facility Security Design  
- Active Assailant

To learn more about ASIS learning opportunities, visit asisonline.org/education.

**BOOK OF THE YEAR**  
At GSX 2018 in Las Vegas, *The Five Technological Forces Disrupting Security* was named the ASIS Security Industry Book of the Year. Author Steve Van Till, CEO of Brivo, spoke to Security Management about the book and the award.

**Q. What do you hope readers will learn from your book?**  
**A.** First, technological forces are creating changes in security at a faster pace than ever before, and we need to embrace them in order to keep pace with larger context in which we are protecting people and assets. Second, much of this change can be attributed to the effects of consumer adoption of both the IT and security technologies at our disposal. Think of mobile communications, for example, and what it has meant for both convenience and situational awareness. The Internet of Things, which is a newer technology, gives us increasing amounts of data as it becomes more widely deployed. Finally, education and training are critical, because tools don’t do anything until they are in the hands of someone who knows how to use them. That’s one of the great things about the role of GSX in the industry, and why I’m especially honored to receive this recognition from a group so dedicated to learning.

**Q. What are the challenges facing our profession today?**  
**A.** I start with recruitment and retention...
because without the right people, we can’t prevail, and the talent wars are at a peak right now. None of the new technologies I talk about in the book will manage themselves, and to be useful they need to be applied to the specific risk management needs of each organization.

Information security is an underlying challenge to everything we are trying to accomplish with technology, because every security technology must necessarily be secure from cyberattack. Information security is a people problem— one that only the right people can solve.

Q. What does the award mean to you?
A. Broadly, the award means that this set of topics resonates with the concerns of security practitioners. That’s important because the natural conservatism of our industry has often meant hanging back a bit on technology decisions. But there’s no longer any room for that because both the risks and the opportunities are too great to ignore. On the risk side, no one can operate without a cyber defense plan, and that means understanding all the technologies that can be used for attack or defense. On the opportunity side, big data and analytics are among the best risk mitigation tools that have ever come along.

Hear more from Steve Van Till in this month’s Security Management podcast. The book can be purchased from the ASIS store at asisonline.org.

LIFE MEMBER
ASIS congratulates Roger B. Maslen, CPP, on becoming a Life Member. He has been an ASIS member for more than 29 years. During that time, he has been active with the Calgary/Southern Alberta Chapter, where he has served as chapter chair, vice chair, treasurer, and secretary. Maslen has also been an ASIS regional vice president and senior regional vice president. He was a member of the Professional Certification Board for several years and is a Lifetime CPP.

MEMBER BOOK REVIEW

Security practitioners looking to learn about physical access control systems can find what they’re looking for in the second edition of Electronic Access Control. The book addresses basic access control concepts that each security practitioner should know, as well as advanced designs and technologies related to physical access control.
The author uses a simple structured approach to address concepts, designs, and technical challenges in layers to ensure a smooth buildup of knowledge. Because it addresses design and functional specifications, as well as operational challenges, the book is an excellent reference for security engineers, security system designers, maintenance technicians, and security operations leaders.

The book contains in-depth information about access control system designs, readers, doors, locks, and the backend software that governs the system. This second edition has added a focus on biometrics, new technologies (locks, network devices, and alarm and video integration), cloud-based systems, and open source solutions.

Besides addressing design and equipment requirements, the book also discusses vulnerability of existing designs and systems. It takes on important concepts that are often overlooked in security systems, such as force multipliers and integration. Moreover, the book successfully relates the architectural design of the facility and the proposed access control system. This link can make or break an implementation of an access control system at any operational facility.

Author Thomas Norman, CPP, PSP, has created a useful technical and operational guide for security access control systems. This detailed book is well organized, with chapter summaries that emphasize the important points, and can serve as a valuable reference for security professionals.

**REVIEWER:** Khalid Al-Ghamdi, CPP, PSP, is the head of security engineering and projects for Saudi Aramco. He is an ASIS Petrochemical, Chemical and Extractive Industry Security Council member and an assistant regional vice president for ASIS Region 12A.

**CERTIFICATION PROFILE**

**NIKILESH SHARMA, CPP, PCI, PSP**

Whether it’s baseball, horse racing, or certifications—the Triple Crown is a rare accomplishment. Fewer than 200 security professionals worldwide have completed the ASIS board certification Triple Crown: Certified Protection Professional (CPP®), Physical Security Professional (PSP®), and Professional Certified Investigator (PCI®) designations. Nikhilesh Sharma, CPP, PCI, PSP, earned them all in just 18 months.

Before working in private security, Sharma served more than 20 years in the Indian military, supporting the army in logistics and planning roles. “With my military background, security was part of my bread and butter,” he says. “As I transitioned out of the army, I sought a job in security management—similar to my previous roles, but in a different setup with new considerations.”

During a security management reset course, his instructor mentioned ASIS certification as a means of strengthening his security background. Sharma was working in security and facility management with the Residential Welfare Association (RWA) for the Gurjinder Vihar township in Greater Noida, India, so he spoke with certification holders from nearby ASIS chapters. He saw the value of this professional organization and joined the New Delhi Chapter in February 2016. Then he set out on his certification journey.

“Guided by the exam domains, the Protection of Assets, and ASIS standards and guidelines, I woke up and studied between 4:00 a.m. and 7:00 a.m. each weekday, with two more hours of study upon returning home in the evening,” he notes. “On Saturday, I would evaluate my progress against my study goals, and then take a break on Sunday to refocus on the week ahead.”

He attained the CPP in July 2016—and set his sights on the PSP and PCI.

He found an online study group and earned the PSP in August 2017. Just five months later, he obtained his PCI designation and took over as chief security officer for luxury hotel ITC Rajputana. He has recently moved to the Toronto, Canada, region.

“Once I earned my certifications, I enjoyed additional responsibilities in all my assignments,” he notes. “The knowledge gained from exam preparations also helped improve my security practice against current threats. After having acquired all three certifications, I was able to show my company the benefits of employee certification. The company created a policy to sponsor more security managers to attain their CPP certifications.”

Sharma’s recommendation for ITC staff to become certified echoes his greater commitment to the security community and professional development. He spearheaded a program to encourage guards at the company to specialize and diversify their skill sets. “I built a training schedule,” he says, “and in a matter of months our security guards learned skills, including metal detector machine operation, concierge duties, and security operations center and visitor management system operations.”

Regarding studying, he recommends the following: “Chart your progression through the study material and stay focused as you prepare. Your certification is an investment in your future. Reach out to local ASIS chapters, and, if possible, keep in touch with a mentor. Do not give up. Stick to your daily work schedule, and it will only be a matter of time before you have the certifications under your belt.”

PROFILE BY STEVEN BARNETT, ASIS COMMUNICATIONS COORDINATOR
ELSEWHERE IN THE COURTS

JUDICIAL DECISIONS

SURVEILLANCE. An employer’s video surveillance policy of filming employees distributing union materials and literature is illegal, according to a recent ruling by the U.S. National Labor Relations Board (NLRB).

In March 2015, employees of AdvancePierre Foods, Inc.—an Ohio-based corporation that manufactures processed foods for convenience stores and restaurants—contacted a union about unionizing the company’s employees.

A few months later, some employees began distributing union literature and authorization cards at or near the AdvancePierre plant. Some employees complained to management about the distribution effort, which was occurring in the company breakroom.

AdvancePierre management reviewed video surveillance of the breakroom and confirmed that employees were distributing union materials in that space in violation of company policy. The two employees engaged in the activity were questioned, reprimanded, and warned not to distribute union literature again.

The union filed a claim on behalf of the employees with the NLRB. The

TRADE SECRETS

Belgian authorities arrested Chinese operative Yanjun Xu and extradited him to the United States where he faces charges of conspiring and attempting to commit economic espionage and steal trade secrets from aviation and aerospace companies.

Yanjun Xu is a deputy division director with the Chinese Ministry of State Security. He allegedly targeted companies inside and outside the United States—including GE Aviation—by identifying experts who worked for these companies to recruit them to travel to China under the guise of delivering university presentations, according to the U.S. Department of Justice. (EEOC v. Sherwood Food Distributors, LLC, U.S. District Court for the Northern District of Ohio Eastern Division, No. 1:18-cr-00043-TSB, 2018)

DISCRIMINATION

Sherwood Food Distributors, LLC, will pay $3.6 million and provide other relief to settle a class sex discrimination lawsuit filed by the U.S. Equal Employment Opportunity Commission (EEOC). The lawsuit alleged that “Sherwood discriminated against a class of female applicants at its warehouses in Cleveland, Ohio, and Detroit, Michigan, by refusing to hire them for entry-level positions because of gender.” As part of the consent decree, Sherwood will offer jobs to at least 150 women identified during the claims process, implement hiring goals to increase the percentage of females hired for entry-level warehouse positions, and maintain a higher representation of females in those positions over time. (EEOC v. Sherwood Food Distributors, LLC, U.S. District Court for the Northern District of Ohio Eastern Division, No. 1:16-cv-02386, 2018)

DISCRIMINATION

SMS Group Inc. will pay up to $62,000 to resolve charges that it engaged in disability and genetic information discrimination. In an EEOC investigation, the agency found reasonable cause to believe that one of the company’s facilities contracted with a third-party medical provider to conduct medical and fitness-for-duty examinations after employment offers were made. During these exams, applicants and employees filled out questionnaires about their medical history—including cancer, diabetes, heart disease, and stroke—an alleged violation of the Genetic Information Non-Discrimination Act.

LEGAL ON THE HILL

ISSUE: Firearms
BILL: Initiative 1639
VENUE: Washington
STATUS: Passed
SIGNIFICANCE: Raises the age to buy semi-automatic rifles to 21; enhances background checks, training requirements, and waiting periods for purchasing firearms; and creates a storage law.

ISSUE: Marijuana
BILL: Proposal 1
VENUE: Michigan
STATUS: Enacted
SIGNIFICANCE: Legalized the possession and use of recreational marijuana for adults 21 years or older.
case went before an administrative law judge, who found that AdvancePierre violated sections of the National Labor Relations Act (NLRA).

These violations included “maintaining an unlawful no-solicitation/no-distribution policy; surveilling, interrogating, and disciplining four employees for engaging in protected union activity; and soliciting grievances from employees,” according to the NLRB.

The case later went before an NLRB three-judge panel, which came to the same conclusions as the administrative law judge. It also found that AdvancePierre’s decision to use video surveillance to confirm a violation of an illegal policy was an unlawful use of surveillance of employees.

As part of the NLRB’s order, AdvancePierre is required to desist its policy of no-solicitation/no-distribution, engaging in surveillance of employees’ union activity, interrogating employees about their union activities or those of coworkers, and more. (AdvancePierre Foods, Inc., and United Food and Commercial Workers Union, NLRB, No. 09-CA-153966, 2018)

ARBITRATION. Employers cannot require job applicants or employees to sign mandatory arbitration agreements as a condition of their employment, according to a ruling by the Kentucky Supreme Court.

The ruling stems from a case brought by Danielle Snyder, an administrative purchasing agent who was forced by the Northern Kentucky Area Development District (NKADD) to sign an arbitration agreement for any potential disputes with NKADD as a condition of continuing her employment.

The agreement allowed Snyder to revoke her acceptance “by communicating your rejection in writing to the District within five days after you sign it,” according to court documents. “However, because the agreement is a condition of employment, your employment and/or consideration for employment will end via resignation or withdrawal from the process.”

Snyder filed a claim in a trial court under the Kentucky Whistleblower Act (KWA) and the Kentucky Wages and Hours Act, alleging NKADD’s mandatory arbitration agreement was a violation of a Kentucky statute.

The Kentucky Revised Statute prohibits employers from conditioning employment on an existing employee’s or prospective employee’s agreement to “waive, arbitrate, or otherwise diminish any existing or future claim, right, or benefit to which the employee or person seeking employment would otherwise be entitled,” the suit said.

Through a series of court proceedings, Snyder’s case reached the Kentucky Supreme Court. NKADD had appealed a lower court ruling, arguing that the U.S. Federal Arbitration Act “broadly prohibits discrimination against arbitration agreements” and that the federal act “preempts” the Kentucky Revised Statute, according to court documents.

The court, however, was not convinced by NKADD’s argument and ruled in Snyder’s favor.

“We conclude that Kentucky state-created entities do not have the power to compel, as a condition of employment, any employee to agree to arbitrate any claim, right, or benefit he or she may have against NKADD,” the court wrote in its opinion. “Although NKADD appears to have broad power to enter into agreements and define the terms of those agreements, [the Kentucky Revised Statute] expressly prohibits NKADD from conditioning employment on an agreement to arbitrate.” (Northern Kentucky Area Development District v. Snyder, Supreme Court of Kentucky, No. 2017-SC-000277-DG, 2018)

LEGISLATION

Australia

ENCRYPTION. Australian legislators are considering a bill that would weaken encryption standards in the country and require private sector cooperation.

The Assistance and Access Bill 2018 would amend the Telecommunications
Act of 1997 to allow police forces and anti-corruption agencies to ask—and then require—Internet companies, telecommunications providers, messaging providers, and others to access content they have requested. This would apply even to data that is encrypted, and requests would not be subject to judicial review.

The bill would allow service providers to refuse to provide access if providing access to the requested data would violate another nation’s laws.

As of press time, the bill is in the committee stage in the House of Representatives and was introduced to address national security and law enforcement challenges.

“Australian national security and law enforcement agencies are facing increasing difficulties in accessing encrypted communications that mask a variety of illegal activities,” said Andrew Hastie, chair of the Australian Parliamentary Joint Committee on Intelligence and Security, in a statement. “The bill provides national security and law enforcement agencies with powers to respond to the challenges posed by the increasing use of encrypted communications and devices.”

Critics, including major U.S. technology firms, claim that the legislation lacks transparency and infringes on Australian privacy rights.

“We are pleased that some of the suggestions incorporated improve the legislation, the unfortunate fact is that the draft legislation remains dangerously ambiguous with respect to encryption and security,” Apple said in a letter to the Australian parliament. “This is no time to weaken encryption. Rather than serving the interests of Australian law enforcement, it will just weaken the security and privacy of regular customers while pushing criminals further off the grid.”

**United States**

**INFORMATION SECURITY.** U.S. President Donald Trump signed legislation into law that requires the Surface Transportation Board (STB) to implement information security recommendations.

The recommendations in the law (P.L. 115-269) require STB to “identify controls, including risk management, weakness remediation, and security authorization; to protect controls, including configuration management, user identity and access management, and security training; to detect controls, including incident handling and reporting; to recover controls for contingency planning; and any additional tools that will improve the implementation of the recommendations.”

STB is also required to annually report to congressional oversight committees on its progress and implementation of the recommendations.

The recommendations were originally made in a U.S. Department of Transportation inspector general report that found that STB’s original information security program was “not effective,” increasing its “susceptibility to external threats and to non-compliance with federal requirements and guidelines.”

U.S. Representative Paul Mitchell (R-MI) introduced the original legislation.

**SUPPLY CHAIN.** The U.S. Senate Homeland Security and Governmental Affairs Committee advanced legislation that is designed to enhance supply chain security.

The bill (S. 3085) would create a Federal Acquisition Security Council made up of representatives of the Office of Management and Budget, the General Services Administration, the Department of Homeland Security (DHS), the Office of the Director of National Intelligence, the FBI, the Department of Defense, and the National Institute of Standards and Technology.

This council would develop criteria and processes to assess threats and vulnerabilities related to supply chain risk, share information among agencies on that risk, develop standards and measures for supply chain risk management, and other responsibilities.

The bill was introduced by U.S. Senator Claire McCaskill (D-MO) and has one Republican cosponsor, U.S. Senator James Lankford (R-OK).

The legislation was created after the Trump administration submitted a legislative proposal to Congress to address supply chain risk poses by the acquisition of information technology, along with an annual report to the appropriate congressional committees on the council’s activities.

The bill was introduced by U.S. Senator Claire McCaskill (D-MO) and has one Republican cosponsor, U.S. Senator James Lankford (R-OK).

The legislation was created after the Trump administration submitted a legislative proposal to Congress to address supply chain risk poses by the acquisition of information technology, along with an annual report to the appropriate congressional committees on the council’s activities.

The bill was introduced by U.S. Senator Claire McCaskill (D-MO) and has one Republican cosponsor, U.S. Senator James Lankford (R-OK).

The legislation was created after the Trump administration submitted a legislative proposal to Congress to address supply chain risk poses by the acquisition of information technology, along with an annual report to the appropriate congressional committees on the council’s activities.

The bill was introduced by U.S. Senator Claire McCaskill (D-MO) and has one Republican cosponsor, U.S. Senator James Lankford (R-OK).
REACH NEW HEIGHTS in Professional Excellence

ASIS accredited certifications can help you reach your career goals.

“ASIS board certification offers tremendous credibility and accountability. Combined with its accompanying continuing education requirement, it is a great way to demonstrate security expertise.”

—Pamela Cichon, CPP, Program Manager, United States Postal Inspection Service

asisonline.org/cert
INDUSTRY NEWS  | BY FLORA SZATKOWSKI

GAMES STRATEGY

THE 18TH ASIAN GAMES kicked off in August 2018 in Jakarta and Palembang, Indonesia. NUCTECH provided security inspection equipment, which was installed in the office of the organizing committee, the Athletes Village, and the athletic venues. Vehicle-scanning equipment inspected logistics vehicles entering the Athletes Village.

Two technical service teams in two host cities ensured that nothing went wrong. In addition to the equipment used at the venues of the Asian Games, NUCTECH security equipment was operational at the Soekarno–Hatta International Airport to ensure the safety of delegations from all countries.

AWARD

The Counterterrorism Education Learning Lab and the Minneapolis Police Department received the International Association of Chiefs of Police Booz Allen Hamilton Leadership in the Prevention of Terrorism Award for success in countering terrorist activity. This year’s award recognized community training in advance of Super Bowl LII.

CONTRACT

Teleste Corporation announced that its S-AWARE platform was chosen by Helsinki City Transport to drive situational awareness and safer traveling in the metro system. The platform collects information from various inputs and displays a unified view of operations.

ANNOUNCEMENT

ONVIF announced the final release of Profile T, a new specification with advanced video streaming capabilities and an expanded feature set for metadata streaming and analytics. Profile T also offers support for H.265 video compression.

PARTNERSHIPS

EVENT MANAGEMENT
Johnson Controls and Everbridge will collaborate to provide a platform to rapidly notify stakeholders in active shooter situations with event details and instructions.

ACCESS INTEGRATION
IndigoVision is integrating alarms from TDSi systems for video and alarm management in a single user interface.

AUTHENTICATION
Raptis Rare Books is using technology from SelectaDNA to authenticate literary works.

CARGO SECURITY
Evotec chose Idesco readers for its cargo security system. The readers are installed on transport company vehicles.
WHEREVER YOU ARE

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

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

**MAGAZINE**
Read the award-winning print publication from ASIS International.

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

**SOCIAL**
Join the discussion on Facebook and Twitter.

**PODCAST**
Hear what security professionals are talking about.

**E-MAIL**
Subscribe to the SM Daily and Weekly Newsletters.
RARITAN of Somerset, New Jersey, introduced an intelligent electronic door access-and-control system that supports all types of data center cabinets and enclosures. The easy-to-install SmartLock system safeguards the server cabinet and its residing data by managing the physical access to the cabinet and keeping a digital log of all activity. Data center managers can use the SmartLock system to lock and unlock cabinet doors, check the status of a cabinet door, authorize user access, define alert settings, and generate a digital audit trail report. SmartLock installs into any IT cabinet door, eliminating the cost of installing a separate security system, wiring, and network cabling. It plugs directly into Raritan’s intelligent rack power distribution units or EMX Smart Rack Controllers residing in cabinets and integrates with their IP network and management dashboards.

MIDDLE ATLANTIC PRODUCTS of Fairfield, New Jersey, introduced the latest innovation within its universal DC Power Distribution family. Available for North American and European installations, the new 200W and 300W models provide high current capacity to up to 24 devices, maximizing the same voltage in a single unit or splitting between 12 and 24 volts. They eliminate power-cabling clutter caused by the growing number of small devices within installations. The solutions’ reliable multilevel protection on both AC input and DC outputs and built-in individual redundancy ensure maximum uptime.

SOTER TECHNOLOGIES of Hauppauge, New York, announced a significantly enhanced model of its innovative Fly Sense detection system, which detects vaping and sound anomalies in areas where cameras are prohibited. New and enhanced features for Fly Sense 2.5 include state-of-the-art vape sensor technology, a mobile app, status indicator LEDs, alert scheduling features to make monitoring and response easier, and robust analytics based on incident alert history. It can monitor and detect sounds that could indicate fighting or bullying is occurring. When vaping or elevated sound is detected, school officials are notified by text message, email, or through the mobile app.
Los Angeles-based SWANN launched Google Assistant voice control on its multicamera wired surveillance systems. Users can use voice commands to stream video from security cameras to a TV using the Google Assistant via Google Home and Chromecast. While some wireless cameras have incorporated voice integrations, this is the first time wired multicamera systems have that option. Wired systems remain more robust and secure compared to their wireless counterparts and can offer users a view of multiple cameras on their TV with a simple voice command.

**Wireless Extender**

LUXUL of Draper, Utah, offers the new P40 AC1200 WiFi Bridge + Range Extender. The P40 features 802.11ac dual-band technology to deliver data rates up to 1200 Mbps (300 Mbps on 2.4 GHz band and 867 Mbps on 5 GHz band). Easy to install and configure, it can function as either a bridge link or as a range extender. In Client mode, while acting as a bridge, devices that don’t have built-in wireless capability can be physically connected to the P40, thus connecting them directly to the wireless network. In Repeater mode, while acting as a range extender, wireless connectivity is rebroadcast to remote areas extending a strong signal to weak areas.

**Barriers & Security Bollards**

Protecting what MATTERS MOST.

For product info #23 securitymgmt.hotline.com
TOTAL RECALL CORPORATION of Suffern, New York, a Convergint Technologies Company, introduced a new portable CrimeEye LPR License Plate Recognition unit. CrimeEye LPR includes an Automatic License Plate Recognition (ALPR) camera, emergency battery backup, Wi-Fi, and pole mount. Thanks to its all-inclusive design, the unit can be quickly attached to a street pole in an area of interest and instantly stream captured data to a command center. With such portability, police departments can have an audit trail of passing traffic, alarm on vehicles of interest, and help reduce crime.

CAMERAS AND NVRS

The Wisenet Q series is a new line of affordable cameras and NVRs from HANWHA TECHWIN AMERICA of Teaneck, New Jersey. The professional product line is ideal for small to medium-sized applications. Cameras are available in 24 indoor and outdoor dome configurations and in 2MP and 4MP resolutions. They feature multiple lens options, improved bandwidth efficiency, and built-in infrared. The QRN NVRs provide high-performance recording solutions for smaller installations such as offices and retailers. They can support the display of ultra-high definition 4K display images via their HDMI output ports and support Hanwha’s WiseStream compression technology. By using the metadata from the cameras, the NVRs can improve the searching methods of the archived videos.

ENTRANCE CONTROL

The new DoorGuard system from ORION ENTRANCE CONTROL, INC., of Laconia, New Hampshire, uses light detection and ranging (LIDAR) technology that is a key component in autonomous motor vehicles. The core component of the DoorGuard system is the S3 sensor developed by QUANERGY of Sunnyvale, California. The DoorGuard unit is mounted above a door and integrates to the access system and Orion’s proprietary Infinity software. It is designed to detect one credit per person and deter unauthorized access. It can detect tailgating and set off warnings if a door is open for too long or has been propped open. In emergency situations when access points need to be open, DoorGuard can accurately count those who pass through.

VIDEO ENCODER

VITEC of Sunnyvale, California, offers the MGW Diamond, a compact and portable quad-channel HEVC and H.264 HD/SD video encoder, which is ideal for field-based applications. Its powerful encoding engine can output up to eight streams simultaneously. It is ideally suited to any multichannel application where stringent size, weight, and power characteristics are demanded. For data-sensitive applications, the MGW Diamond supports KLV/STANAG metadata ingest from various sources, real-time image cropping, video scaling, Forward Error Correction streaming, and JSITC compliant output streams. It packs all the needed capabilities for delivering any type of intelligence, surveillance, and reconnaissance or situational awareness video generated by ground vehicles, manned or unmanned airborne platforms, and marine vessels.

SECURITY MANAGEMENT

CNL SOFTWARE of Ashburn, Virginia, released IPSecurity-Center V5.7. The release updates the physical security information management system with many feature enhancements that increase performance and reduce operational response times in large-scale, multi-sited, and mission critical deployments. It improves the ability to manage across multiple SOCs and GSOCs, keeping the entire operation in harmony using enterprise-wide visualization to support the overall security mission for critical infrastructure and large-scale government homeland security programs. It is more scalable, faster, and more responsive, and it offers new features that help companies comply with Europe’s GDPR.

VIDEO ENCODER

VITEC of Sunnyvale, California, offers the MGW Diamond, a compact and portable quad-channel HEVC and H.264 HD/SD video encoder, which is ideal for field-based applications. Its powerful encoding engine can output up to eight streams simultaneously. It is ideally suited to any multichannel application where stringent size, weight, and power characteristics are demanded. For data-sensitive applications, the MGW Diamond supports KLV/STANAG metadata ingest from various sources, real-time image cropping, video scaling, Forward Error Correction streaming, and JSITC compliant output streams. It packs all the needed capabilities for delivering any type of intelligence, surveillance, and reconnaissance or situational awareness video generated by ground vehicles, manned or unmanned airborne platforms, and marine vessels.

CAMERAS AND NVRS

The Wisenet Q series is a new line of affordable cameras and NVRs from HANWHA TECHWIN AMERICA of Teaneck, New Jersey. The professional product line is ideal for small to medium-sized applications. Cameras are available in 24 indoor and outdoor dome configurations and in 2MP and 4MP resolutions. They feature multiple lens options, improved bandwidth efficiency, and built-in infrared. The QRN NVRs provide high-performance recording solutions for smaller installations such as offices and retailers. They can support the display of ultra-high definition 4K display images via their HDMI output ports and support Hanwha’s WiseStream compression technology. By using the metadata from the cameras, the NVRs can improve the searching methods of the archived videos.

ENTRANCE CONTROL

The new DoorGuard system from ORION ENTRANCE CONTROL, INC., of Laconia, New Hampshire, uses light detection and ranging (LIDAR) technology that is a key component in autonomous motor vehicles. The core component of the DoorGuard system is the S3 sensor developed by QUANERGY of Sunnyvale, California. The DoorGuard unit is mounted above a door and integrates to the access system and Orion’s proprietary Infinity software. It is designed to detect one credit per person and deter unauthorized access. It can detect tailgating and set off warnings if a door is open for too long or has been propped open. In emergency situations when access points need to be open, DoorGuard can accurately count those who pass through.
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.

<table>
<thead>
<tr>
<th>CIRCLE #</th>
<th>PAGE #</th>
<th>CIRCLE #</th>
<th>PAGE #</th>
</tr>
</thead>
<tbody>
<tr>
<td>09</td>
<td>21</td>
<td>14</td>
<td>33</td>
</tr>
<tr>
<td>-</td>
<td>06</td>
<td>18</td>
<td>45</td>
</tr>
<tr>
<td>23</td>
<td>63</td>
<td>24</td>
<td>67</td>
</tr>
<tr>
<td>02</td>
<td>04</td>
<td>13</td>
<td>32</td>
</tr>
<tr>
<td>07</td>
<td>15</td>
<td>19</td>
<td>49</td>
</tr>
<tr>
<td>12</td>
<td>29</td>
<td>16</td>
<td>39</td>
</tr>
<tr>
<td>08</td>
<td>19</td>
<td>01</td>
<td>02-03</td>
</tr>
<tr>
<td>25</td>
<td>68</td>
<td>20</td>
<td>51</td>
</tr>
<tr>
<td>15</td>
<td>36-37</td>
<td>11</td>
<td>25</td>
</tr>
<tr>
<td>06</td>
<td>13</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ADVERTISERS ONLINE

Abloy Security, Inc.
www.abloyusa.com

Altronix Corp.
www.altronix.com

Ameristar Security Products
www.ameristarsecurity.com

Axis Communications
www.axis.com

Detex Corporation
www.detex.com

dormakaba
go.dormakaba.com/PAS-SMMag

DSI (Designed Security Inc.)
www.dsigocom

DSX Access Systems, Inc.
www.dsxinc.com

esri
www.esri.com/ASIS

G4S
www.g4sus

GAI-Tronics Corporation
www.gai-tronics.com

Garrett Metal Detectors
www.garrett.com

Mission 500
www.mission500.org

Research Electronics, Int’l
www.reiusa.net

Safety Technology International, Inc.
www.safetytechusa.com

SDC – Security Door Controls
www.sdcssecurity.com

SecurAmerica
www.securamericallc.com

Special Response Corporation
www.specialresponse.com

TSCM America
www.tscmamerica.com
SECURITY AS NATIONAL DEFENSE

Arthur L. Malcarney, vice president at RCA, emphasized the engineering excellence required by security professionals to defeat their enemies by helping the U.S. government protect the nation. When this precursor to Security Management was published, ASIS was 10 years old and the magazine was in its ninth year.

LOCKS AND KEYS

Timothy J. Walsh was president of ASIS when he wrote this article on the fundamentals of six-pin tumbler locks. During the 1960s, annual seminar attendees topped 500, the ASIS Foundation was incorporated, and membership exceeded 3,000 for the first time.

KEEPING WATCH

Founded in 1878, Detex was known during the early 1960s as the sellers of watch-clocks—mechanical clocks used by security officers to confirm patrols. A vendor partner since the inception of ASIS, Detex advertises in Security Management to this day. Its 21st century offerings are on page 15.
Together we can

Educate

Inspire

Heal

Nourish

Children and families in crisis across the USA need our help – and yours. And as a 501(c)(3) organization, Mission 500 now has even greater flexibility to work with local charities to better support existing and new sponsors and volunteers. But even with over 1000 children sponsored and many acts of charity performed to date, there’s still a great deal of work to be done. Get involved today! Visit mission500.org for more information.

Supporting Families Across America

For product info #24 securitymgmt.hotims.com
DSX SECURITY AT YOUR COMMAND... AND IN YOUR HAND.

The Security Professionals’ first choice for today’s security infrastructure, from one room to multi-location complexes around the world. Our reputation is based on a time-honored tradition of rock-solid quality, premium reliability and integrity of DSX and our network of factory-trained, authorized dealers and support.

When you are staking your reputation on a solution — choose the most powerful and intelligent access control system in the world, choose the total security relationship of DSX Access Systems.

DSX STANDARD SYSTEMS FEATURES INCLUDE:

- Integrated Locksets. Wireless and Hardwired
- High Level Elevator Security with braXes™ Integration
- Can Use Mobile Ready Readers Smart Phone Credentials
- Now Standard Software Features: AES-256 Encryption/DVR Integration Redundant Comm-Server (SQL Only)
- No “Per Seat” Licensing In System Pricing
- New User Interface Tabbed Organization
- Accountability Reports Last Use/Access Level History
- Mobile Initiated Incident Response. Emergency Lockdown Email/Text Notification “Who’s In/Muster” Reporting
- Backward Compatible Hardware. Virtual Environment Friendly