SECURITY
MANAGEMENT
JANUARY 2018
A PUBLICATION OF ASIS INTERNATIONAL

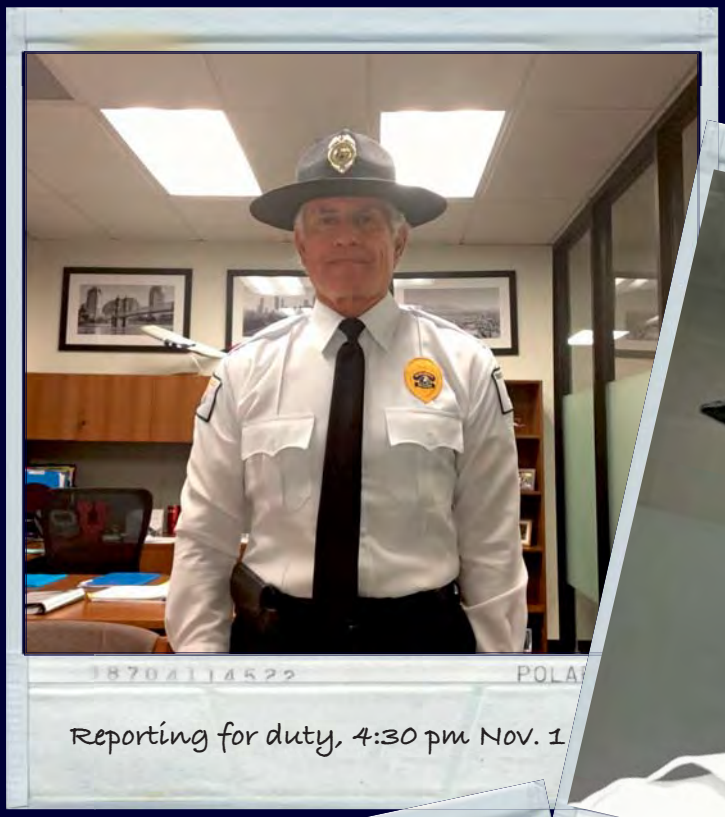
Issue & Beyond

- ***Preparedness***
  Disasters frequently beget more disasters.
- ***Terrorism***
  Companies most at risk for cybercrime are unprepared.

×32

RUN, HIDE, DON'T FIGHT

SECURAMERICA ACQUIRES ERMC



Reporting for duty, 4:30 pm Nov. 1

On patrol, 12:30 am Nov. 2

On patrol, 3:30 am Nov. 2

Ending shift, 6 am Nov. 2

In November, SecurAmerica purchased ERMC, a security and facilities management company based in Chattanooga, Tennessee with $100 million in revenue and 100 locations. SecurAmerica now is a $300 million run rate business with boots on the ground in 500 locations. I believe this makes us the fifth largest security company in the US. And yes, I still own 100%, and yes, we do not have private equity involved with us, just security people.

$1,000,000
CHARITY CHALLENGE: SECURITY GUARD "TAP OUT"

A customer of mine that I have had a relationship with since the 1980s loved my ads and took me up on the challenge of working a post at their corporate office complex. (I apologize for the quality of pictures, but I had to take my own selfies!) This was great training for me for my future Security Guard Tap Out against the Big Four CEOs. I reported to duty at 4:30pm, manned my post and patrolled continually until 6am, when the customers started to arrive for their workday. I stopped by my house to shower and was back at my office by 8am to start my own workday.

Truthfully, staying awake for more than 24 hours straight brought back great memories and was not as tough as I thought it would be! I figure I should be able to go 2 to 3 days straight when the competition begins. I am still waiting to hear from the Big Four CEOs; none of them have accepted my challenge yet for the Security Guard Tap Out.

Since I am in training mode, I could use your help. If you have a national contract for security with one of the Big Four and you are not completely satisfied with their service, please call me, and I will stand guard at your toughest location. Two great things will come from this. First, I get to push myself to see how tough I really am. Secondly and most importantly, when the CEO of your man-guarding company hears I am standing guard for you, I promise you will get more attention from your provider than you've been getting, which is a win-win for both you and me.

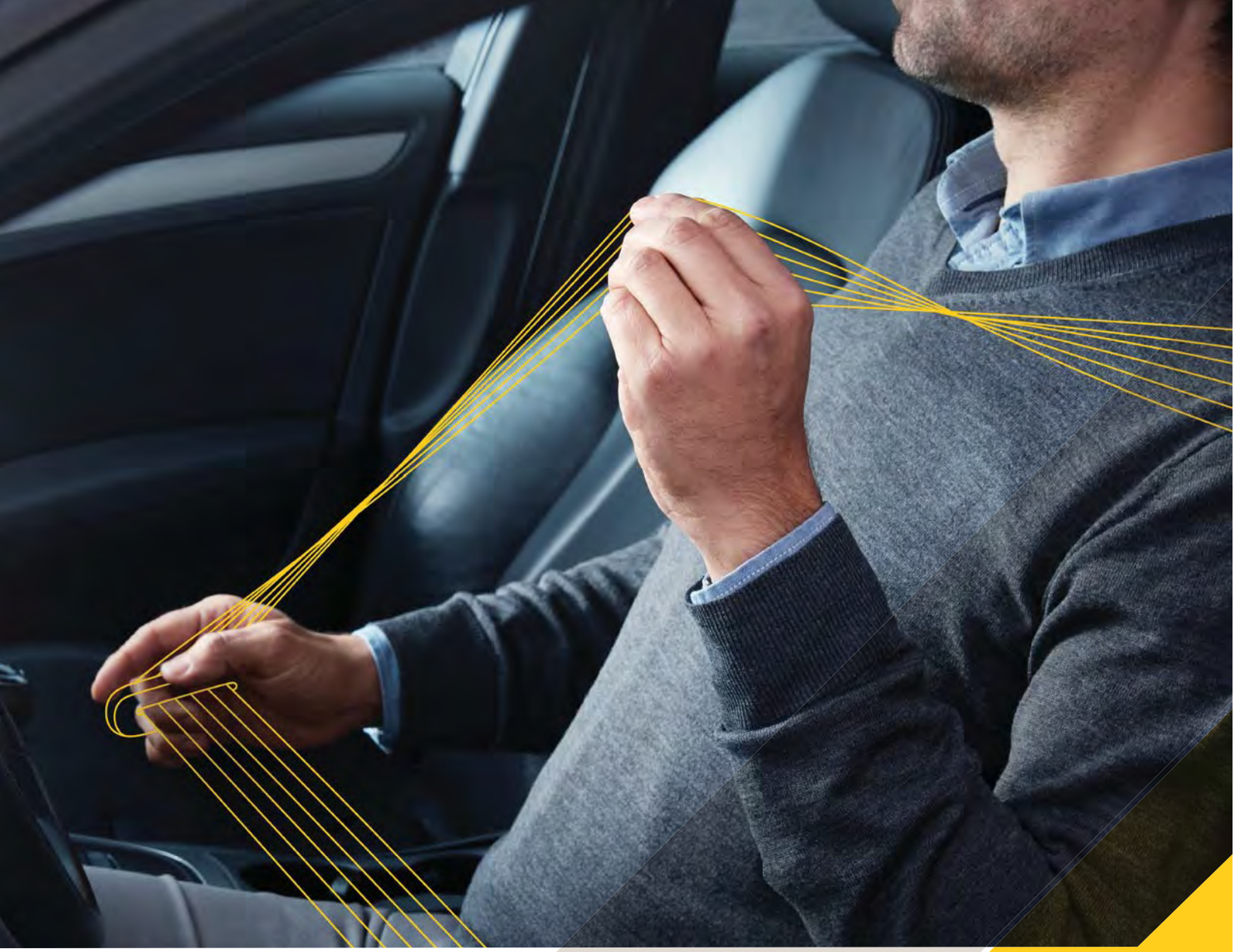
For the first 5 callers that allow me to stand post as requested above, I will donate $10,000 in your name to the ASIS Foundation.

Please call me on my cell at 404-536-1140!

SECURAMERICA

WWW.SECURAMERICALLC.COM

DIRECT LINE: 404-926-4202



Cybersecurity?

Buckle up.

At Axis, we do everything we can to mitigate the risks of cyber attack. We have 100% focus on cybersecurity. We build protection right into your network camera solutions. And we work hard to make it easy for you to play your part. But we really can't do it without you.

Because cyber protection is a lot like the seatbelt in your car. It won't keep you safe unless you use it.

Visit axis.com/about-axis/cybersecurity and find out how to stay protected!

For product info #2 securitymgmt.hotims.com

AXIS COMMUNICATIONS

CONTENTS

NOTABLE

Mia was not a real person, but a carefully crafted online persona created by a prolific group of Iranian hackers.

Scott Stewart, vice president of tactical analysis at Stratfor.com, recounting the means used to perpetrate a malware infiltration of a major accounting firm. PAGE 50

"As we all routinely experience in both our professional and personal lives, success is not something that just happens; it requires a plan and sound execution."

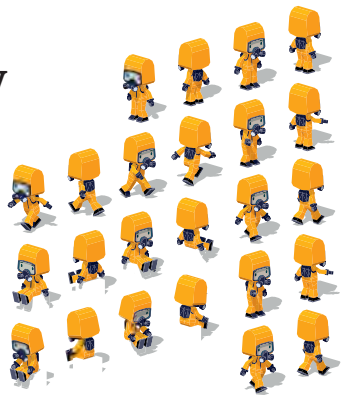
Incoming ASIS President Richard Chase, CPP, PCI, PSP, on the future of ASIS International. PAGE 41

"We went from logging 1,400 different entries on a shift down to 200 just by taking a step back."

Bret DuChateau, corporate security consultant for Northwestern Mutual, on the efficiencies of documenting security events in one system instead of several. PAGE 44

"There are more than two dozen presidentially appointed individuals with biodefense responsibilities."

Christopher Currie, director of emergency management, national preparedness, and critical infrastructure protection at the U.S. Government Accountability Office. PAGE 20



BY THE NUMBERS

44

The percentage of executives who said in a global survey that they do not have an overall information security strategy. PAGE 28

$186B

The preliminary total of damages from the 2017 hurricane season. PAGE 14

30

The number of people injured by a series of bombings in New York City and New Jersey in 2016. The perpetrator was convicted and faces the possibility of multiple life sentences. PAGE 60

ILLUSTRATIONS BY THINKSTOCK

BPA WORLDWIDE

Security Management (ISSN 0145-9406) Volume 62, 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, $162. All others—air delivery—1 year, $120. Bulk subscription rates available. Periodicals postage paid at Alexandria, VA and additional mailing offices. Mailed in Canada under IPM #0743968. Postmaster: Send address changes to ASIS International, Attn: *Security Management*, 1625 Prince St., Alexandria, VA 22314. *Security Management* is a registered trademark and its use is prohibited.

SM

Maximum Reliability...

...Minimum Size!

- ***New*** 56-in. Pedestal
- ***New*** 7-ft. Tower with Strobe
- Accommodates GAI-Tronics ***New*** Compact Series Telephones

GAI-TRONICS®
A Hubbell Company

1-800-492-1212 **www.gai-tronics.com**

JANUARY 2018

ASIS INTERNATIONAL
Advancing Security Worldwide®

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

Michael Gips
chief global knowledge and learning officer
Michael.Gips@asisonline.org

Nello Caramat
publisher
Nello.Caramat@asisonline.org

BUSINESS OFFICES
1625 Prince Street
Alexandria, VA 22314

703/519-6200
fax 703/519-6299

SALES REPRESENTATIVES

Western/Midwestern Sales Representatives
Jeffrey B. Dembski, Steve Loerch
847/498-4520
jeff.dembski@asisonline.org
steve.loerch@asisonline.org

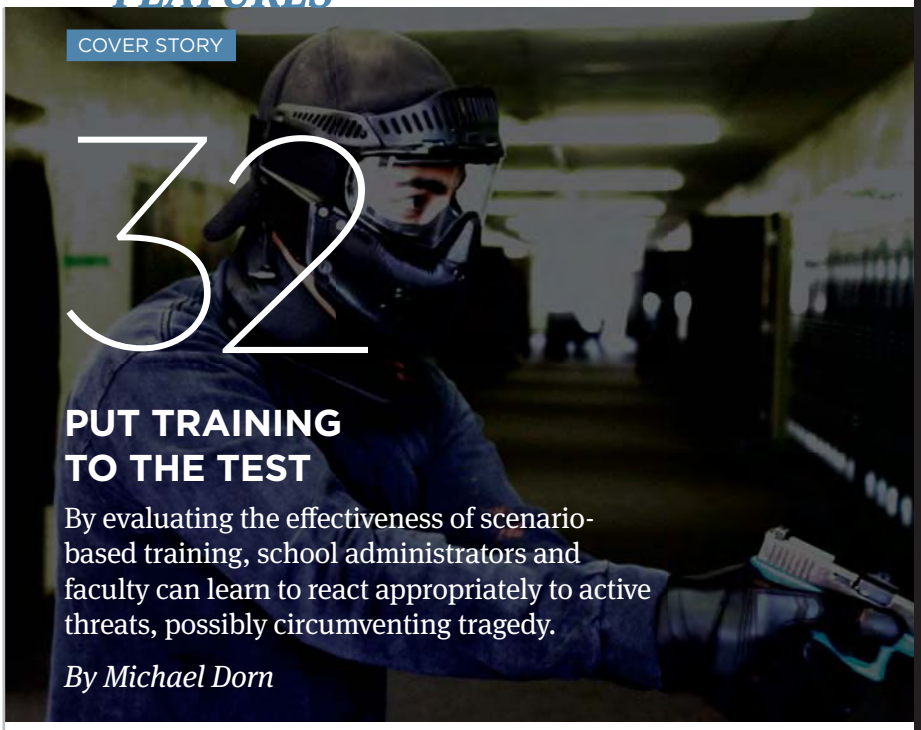
Southern/Mid-Atlantic & Europe Sales Representative
Shawn Register
334/270-4060
shawn.register@asisonline.org

Northeastern Sales Representative
Charlotte Lane
334/239-2218
charlotte.lane@asisonline.org

On the Cover:
Photograph
by Sharon McCutcheon, EyeEm, Getty Images

CONTENTS

FEATURES



SM

ACHIEVE THE HEIGHTS OF SUCCESS

Partner.Win.

It's an exciting time to partner with Hikvision. The world's leading video surveillance manufacturer, we work hard alongside our team members and our partners so that we all win together.

#PartnerWin

hikvision.com

HIKVISION®

For product info #4 securitymgmt.hotims.com

JANUARY 2018

SECURITY MANAGEMENT

EDITORIAL OFFICES

1625 Prince Street
Alexandria, VA 22314
703/519-6200
fax 703/519-6299

EDITORIAL

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

CONTENTS

DEPARTMENTS

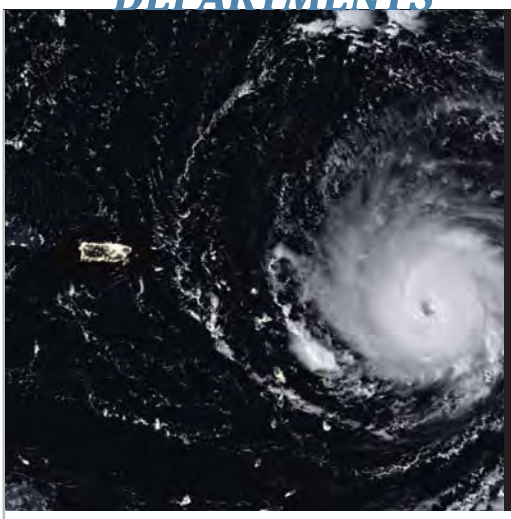


PHOTO BY IRINA DMITRIENKO, ALAMY STOCK PHOTO

CHECK OUT MORE ONLINE at *www.securitymanagement.com*

ONLINE HIGHLIGHT

SCHOOL SAFETY

Campus security nonprofit Safe Havens International offers free school safety resources on its website that can be used in K-12 schools, as well as for higher learning institutions. Documents include a safety plan evaluation tool, a building design checklist, and a sample background investigation booklet for the hiring process. Safe Havens International works with schools on national and international levels in planning, coordinating, and evaluating a wide range of school crisis simulations.

NEW ONLINE THIS MONTH at www.securitymanagement.com

SM ONLINE

EMAIL
The U.S. Department of Homeland Security issued a binding directive that requires all U.S. agencies to adopt email and Web security guards against phishing and spam.

WHISTLEBLOWERS
Financial incentives can discourage whistleblower reporting, according to a new study.

BIODEFENSE
Despite a call for a united biodefense approach, U.S. federal agencies continue to face challenges in sharing threat information, according to a GAO report. A 2016 panel on biodefense contends that the U.S. vice president should lead the nation's biodefense efforts.

BOMBING CONVICTION
A jury convicted Ahmad Khan Rahimi on eight charges related to bombings in New York City on September 17, 2016, which injured more than 30 people.

CYBER STRATEGY
Despite awareness of cyber risks, many companies remain unprepared to deal with them, according to PricewaterhouseCoopers' *The Global State of Information Security Survey 2018*.

CRISIS COMMUNICATION
SmartRiskSolutions GmbH published a handbook with advice for crisis management and communications during a terrorist attack or active shooter incident.

ASIS ACCOLADES
Attendees at ASIS 2017 voted the Pelco by Schneider Electric VideoXpert Professional Video Management System the ASIS Accolades People's Choice Award winner. Read about all the winners.

FIRE SAFETY
The "2016 Fire and Life Safety Study" from *Consulting-Specifying Engineer* surveyed its subscribers on what matters to them when selecting a fire and life safety system.

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

Securing Life - *Put Your Trust In* GARRETT®

PORTABLE PROTECTION, WORLD-CLASS RELIABILITY

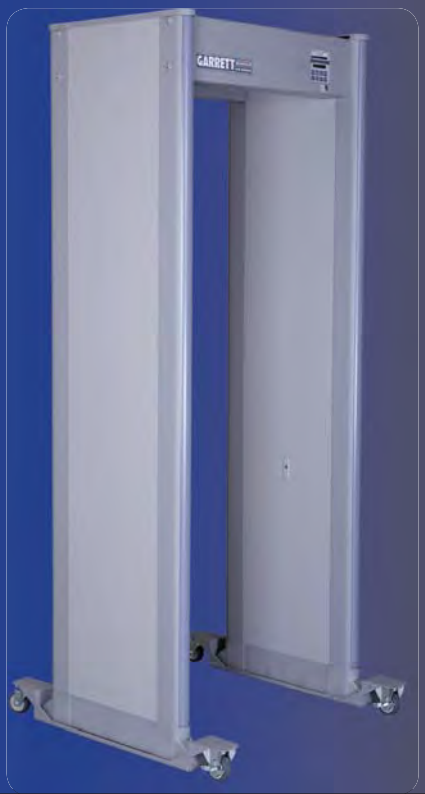
Garrett's PD 6500i walk-through detector offers:

- Superior throughput, with high discrimination of innocuous items.
- Optional caster set enables full mobility for rapid deployment at special events and sports arenas.
- Optional battery modules for continuous operation without power cables or other wiring.

THE GARRETT ADVANTAGE

- Metal detection technology trusted since 1964.
- Walk-through, hand-held, and ground search models designed for all applications.
- Each detector is proudly made in the USA under Garrett's strict ISO 9001 certified Quality Management System.

For product info #5 securitymgmt.hotims.com



GARRETT®
METAL DETECTORS

MADE IN THE USA

ISO 9001 CERTIFIED

GSA Contract Holder

Performance. Protection. Dependability. Since 1964.

garrett.com

Toll Free: 800.234.6151 (U.S. & Canada)

Editor-in-Chief
TERESA ANDERSON

RESOLUTIONS

Blame the Babylonians. The seemingly endless barrage of ads exhorting us to get healthy, save money, and generally improve ourselves took root at least 4,000 years ago when new year's festivities lasted up to 12 days and took place in March. Records indicate that at those new year's festivities, citizens celebrated the planting of crops, pledged allegiance to rulers, and made promises to settle debts.

According to the article "The History of New Year's Resolutions" by Sarah Pruitt in *History* magazine, the tradition resurfaces in the record again with the Romans, who are responsible for moving the celebration to January to honor the two-faced god Janus.

Pruitt writes that "believing that Janus symbolically looked backwards into the previous year and ahead into the future, the Romans offered sacrifices to the deity and made promises of good conduct for the coming year."

We may have moved past planting rituals and public sacrifices, but we seem wedded to the idea of resolutions. People feel compelled to evaluate their past mistakes over the year and strive to do better in the future. Writing for *Psychology Today*, Theo Tsaousides, Ph.D., argues that this is because new year's resolutions are less about tradition and more about the human need to set goals.

Tsaousides explains that this may be simply because setting goals makes us feel good. "Being actively engaged in the pursuit of a goal activates the brain's pleasure centers, independent of the outcome. It seems that we derive more pleasure from chasing our dreams than from achieving them."

But even more importantly, he says, goals provide us with direction. "They give you a destination and enable you to plan your course into your future. Without goals you risk wasting your resources...and being unprepared when opportunities arise."

Volunteer leaders and headquarters staff at ASIS International were certainly dedicated to goal setting, starting new ventures, and being prepared for opportunities in 2017. As 2018 dawns, the fruits of these goals are starting to materialize.

January sees the launch of two major ASIS projects. The association has changed the name of the annual security conference from the ASIS Annual Seminar and Exhibits to the Global Security Exchange (GSX). The newly branded GSX will take place in Las Vegas, Nevada, from September 23 to 27, 2018. Full rebranding details will be announced at the 2018 Leadership Conference this month.

January also sees the launch of phase one of ASIS's new website. The launch is the first part in a multiyear website development project focused on improved and personalized content access, user-centric search and commerce, online community, and integrated systems for learning and certification.

These milestones definitely make those who worked on them feel good, and, as projects evolve, they will generate even more goals. So, maybe the Babylonians were onto something.

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.**

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

DETEX®

DETEX.COM/IMABLUR6

LISTEN • DESIGN • BUILD • SUPPORT

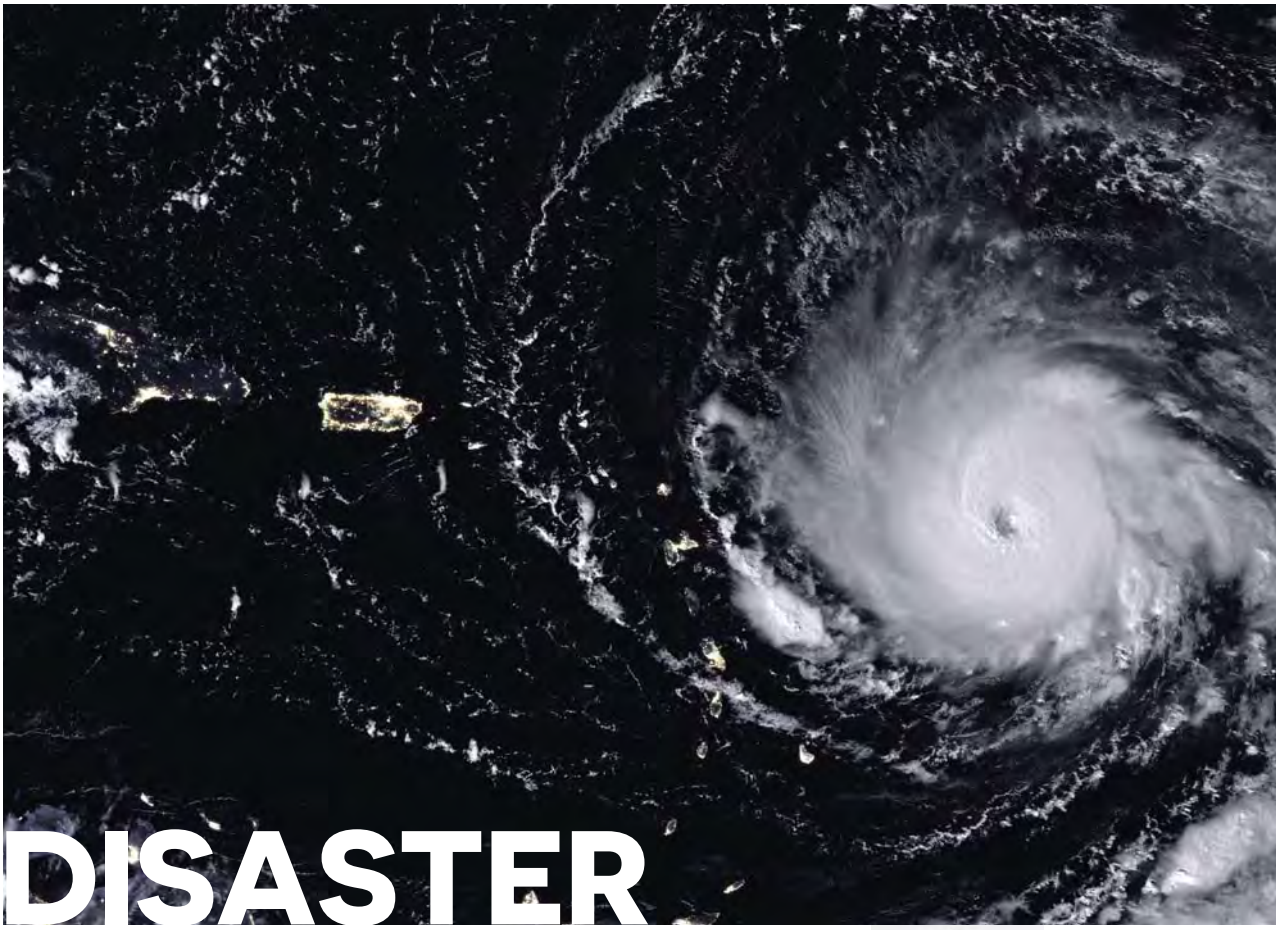


PHOTO BY IRINA DMITRIENKO, ALAMY STOCK PHOTO

DISASTER DOMINOES

THE UNPRECEDENTED 2017 HURRICANE SEASON MADE FOR HARD LESSONS IN EMERGENCY RESPONSE, INCLUDING THE IMPORTANCE OF PLANNING FOR DISASTERS THAT BEGET OTHER DISASTERS.

BY MARK TARALLO

"I'VE BEEN DOING THIS close to 40 years, and there has not, in my career, been a hurricane season anything like this," disaster response expert Jerome Hauer explains in a recent interview regarding the unprecedented 2017 Atlantic hurricane season.

Given his experience base, that is saying something. Hauer has led the homeland security and emergency services department for the state of New York, the office of emergency management in New York City, and Indiana's department of emergency management. On the federal level, he has served as assistant secretary for the U.S. Office of Public Health Emergency Preparedness (OPHEP). He is also a longtime member of ASIS International, and is now a professor at Georgetown University's Center for Security Studies.

But despite all those years in the field, Hauer cannot recall a storm season like the one that just passed. Starting with Hurricane Franklin and ending with Hurricane Ophelia, the 2017 season featured 10 consecutive hurricanes—the greatest number in the satellite era, all of which were marked by winds of at least 75 miles per hour. It may also have been the costliest season on record, with a preliminary total of more than $186 billion in damages, nearly all of which resulted from the three most devastating hurricanes: Harvey, Irma, and Maria.

Each of these massive hurricanes had its own profile. Harvey, for example, came with flooding of biblical proportions, and Irma devastated portions of Florida's power grid. Experts like Hauer say that these two hurricanes illustrated some lessons for emergency preparedness and response. (Experts interviewed for this article did not focus on Hurricane Maria, because the response to that storm was

complicated by political and geographic factors.)

For example, while emergency management leaders in localities and states understand the importance of planning, they do not have the time nor resources to plan for every possible scenario, and so they normally do not plan for the unprecedented—such as three Category 4 hurricanes that make landfall within the span of four weeks.

> ***When you are doing business continuity and disaster planning, in general, you should assume multiple events.***

"This many hurricanes that impact the United States and its territories in a single year is something that you couldn't contemplate," Hauer says. "Particularly since the hurricanes were catastrophic. The strength of the hurricanes, the volume of rain in some areas—we haven't seen anything like this that I can remember."

And even if a sole visionary emergency manager formulated a plan to protect all affected places from an unprecedented hurricane season, in the real world no jurisdiction or state government would have the billions needed to actually implement and fund the required costs of reinforcing, rebuilding, or replacing the various infrastructure systems that would be affected, says emergency management expert Harry Rhulen. Rhulen is CEO of the crisis management firm Firestorm and a member of the ASIS International Crisis Management and Business Continuity Council.

Nonetheless, the series of devastating hurricanes did illustrate another emergency management lesson, Rhulen says: proper disaster preparedness and response means planning for multiple disasters, not just one. "It's one of the most important things to account for—when you are doing business continuity and disaster planning, in general, you should assume multiple events," Rhulen says.

Indeed, Hauer says that's a critical element of disaster response management—planning for the potential second- and third-level disasters. "We did that on a regular basis, both when I was in federal government and on the city level," Hauer says. "You can't just say we have flooding, and say how you deal with the flooding, but also how you will deal with the secondary effects, such as the health effects."

For example, during Hurricane Sandy, mosquitoes used overflowing reservoirs as a breeding ground, running the risk of the spread of West Nile virus. Similarly, after Hurricane Harvey, flooding in Houston raised the risk of health issues stemming from human contact with floodwater, which can harbor bacteria, viruses, and fungi.

Potential health risks like this mean that environmental experts from groups like the U.S. Army Corps of Engineers should be "part of the process" in disaster preparation, Hauer says. It is also important that hospitals take seriously the requirement to hold emergency exercises and drills. "Some take it seriously, but some don't, and they just go through the motions," he explains. And whether it be a locality or a state, drills by emergency personnel should be critiqued by elected officials who should ask some "tough questions" afterward, he adds.

Another challenge in dealing with cascading disasters is that "the first crisis lowers your ability to perform all of the functions that you normally perform," Rhulen says. For example, a fire that destroys some computer hardware can hinder a company's efforts to protect itself from cyberattacks. And storm damage can increase vulnerability to thievery or other types of criminal activity. "You automatically have to bump up security," Rhulen says.

In addition, resources are finite, so in the case of responding to Hurricane Harvey's effects in Texas, "it stretches resources to the point where you are way behind, and near the breaking point," Rhulen explains. This could hamper the response to any disaster that happens in the near future. "It makes their overall exposure for the next year go up dramatically," he says.

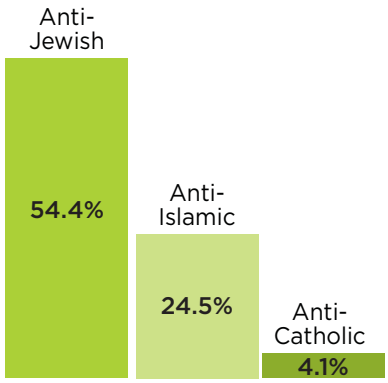
Given that government resources were stretched thin by the double blow of Harvey and Irma, the active volunteer response during the storms was especially critical and "really impressive," Rhulen says. These volunteers, ranging in scope from formal groups to neighbors helping neighbors, beefed up a responder workforce that would have been inadequate without them. "People need to understand—you're really your own first responder," he says.

In the future, the unprecedented hurricane season of 2017 may be

HATE CRIMES

There were 1,584 reported anti-religious hate crime incidents in the United States in 2016. The top three religious biases are depicted here. The remaining 17 percent include crimes against Christians, Hindus, Sikhs, Buddhists, and Atheists.

Targeted Bias (Percent of Total Anti-Religious Hate Crimes)



SOURCE: *2016 Hate Crime Statistics,* FBI, November 2017

looked upon for another historically significant feature. It elicited an unusual type of response—and one that may serve as a closely watched model of resiliency planning in the future—by the island nation of Dominica.

Maria was the worst natural disaster in the country's recorded history. With sustained winds of nearly 160 miles per hour, the storm made landfall on September 19, 2017, as a Category 5 hurricane, forcing the majority of the country's 72,000 residents into homelessness and leaving the island without communication for more than 30 hours. More than 90 percent of the population was left without food, power, or shelter.

In the wake of this devastation, Prime Minister Roosevelt Skerrit said that he does not want to build on old vulnerabilities, but instead develop a targeted resilience strategy so that Dominica becomes the first "climate resilient" nation. "Our desire [is] to be the captains of our fate, and to choose the shape of our recovery," Skerrit said in a statement after the storm.

To do so, Dominica would have to rebuild so that its infrastructure could withstand the type of extreme weather events that may become more common due to climate change. Exactly how the country would do that, and how it could fund such an undertaking, is not yet clear. But Dominican officials are appealing to global organizations for future assistance, and they say that they may have some international partners in their venture.

"The World Bank and European Development Agency have pledged considerable sums to back our vision as the first climate resilient nation of the climate change era," Skerrit said in a recent address to the United Nations General Assembly. "To deny climate change is to procrastinate while the earth sinks."

WHISTLEBLOWING: MONEY V. MOTIVATION

LET'S SAY, as a hypothetical, that a U.S. Internal Revenue Service (IRS) employee blows the whistle on a fraud scheme,

PHOTOS BY THINKSTOCK; *SECURITY MANAGEMENT* ILLUSTRATION

- **Our exclusive canopy options fit single, multiple or space-saving double units.**
- **Power assist is activated with a slight push and adjusts to the speed of the individual entering the turnstile.**

Set your boundaries.

dormakaba full height turnstiles offer a smart solution for securing the perimeter of buildings and property. The modular system presents multiple design configurations, and electronic access control options allow secure passage to authorized personnel.

Setting boundaries makes access in life smart and secure.

For information, design consultation, specifications or installation call 844-773-2669 for comprehensive project support.

DORMA and KABA are now dormakaba. Visit go.dormakaba.com/PAS-SMMag

dormakaba

A minimum threshold feature in whistleblower reporting programs can unwittingly inhibit the timely reporting of smaller frauds.

which allows the agency to recover $3.4 million in revenue that would have otherwise been lost. Under the agency's Whistleblower Informant Award program, that employee may be entitled to receive a cool $1 million reward.

Other U.S. federal agencies, as well as some private sector companies, offer similar financial rewards in their whistleblowing programs, although the amounts and eligibility conditions differ. Some of them have a minimum threshold. For example, the Whistleblower Informant Award program at the IRS requires that the amount in dispute must be at least $2 million before a reward is paid.

The goal of these financial incentives is to encourage the reporting of unethical and illegal activity, and the financial rewards may seem like an attractive incentive. But a group of academics wondered if the incentives could lead to unintended consequences, in accordance with the behavioral theory of motivational crowding.

Motivational crowding describes how, in certain contexts, extrinsic motivators can also act as disincentives by hijacking one's intrinsic motivation. Under this theory, a sizable financial reward can shift a whistleblower's motivation—instead of reporting on fraud because it's the right thing to do morally, the whistleblower becomes motivated primarily by the financial gain of the reward. Although there may be nothing wrong with that type of motivation per se, in situations when reporting wrongdoing will not result in a financial reward, a potential whistleblower motived by money might be less likely to report.

And so, in *Hijacking the Moral Imperative: How Financial Incentives Can Discourage Whistleblower Reporting*, researchers Leslie Berger, Stephen Perreault, and James Wainberg conducted a study of 166 graduate accounting students, presenting them with various scenarios and vignettes. The responses were measured and studied.

The results were consistent with the researchers' predictions. Study participants assessed a higher likelihood that fraud would be reported in situations where the whistleblower would receive a financial reward. This result suggested that financial rewards can be an effective mechanism to encourage whistleblowing in certain contexts.

But the study also found that when the size of the fraud was less than the prescribed minimum threshold in the whistleblower program, participants assessed a lower likelihood that the fraud would be reported in a timely manner. "As such, we demonstrate that including a minimum threshold feature in whistleblower reporting programs can unwittingly inhibit the timely reporting of smaller frauds," the authors write.

This is not good news, the authors conclude. "This finding is especially problematic since the early detection of fraud is a critical factor in minimizing potential damages and securing access to evidence," the authors write.

See SM Online to obtain a copy of the whistleblower study.

BOOK REVIEW

HUMANE POLICING

BY DARRON SPENCER. Inspire On Purpose Publishing; available from Amazon.com; 224 pages; $19.95.

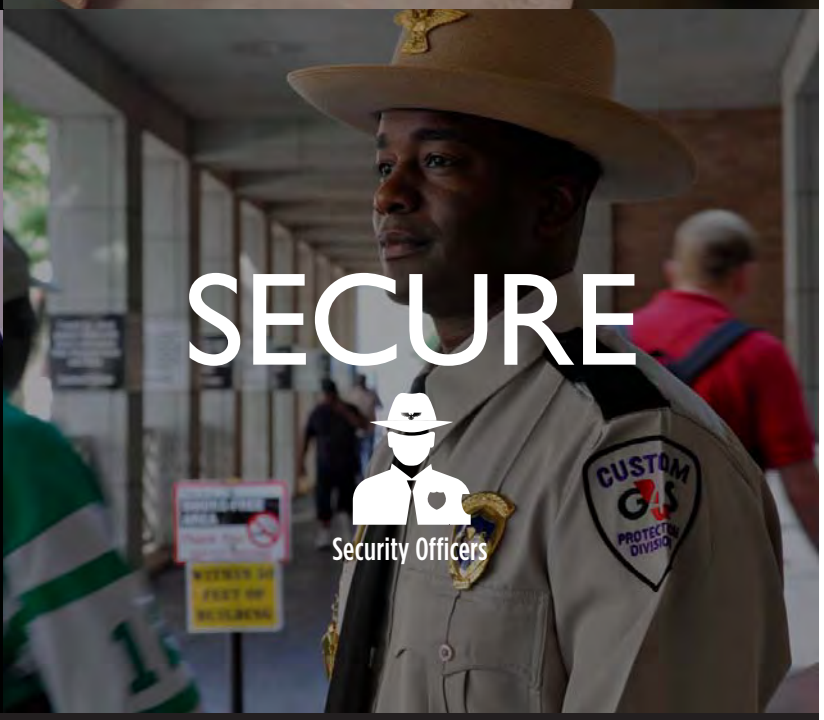
THE LAW enforcement profession has been experiencing a lot of criticism lately, due in part to a small percentage of police officers who choose not to follow the rules. While this is not unique to policing, it sheds light on the festering problems. Author Darron Spencer's *Humane Policing: How Perspectives Can Influence Our Performance* is a well-written quasi-autobiography of one man's experience as a U.S. Marine and sheriff's officer. It advances a new philosophy of community policing and police tactics.

The author chronicles what he learned from the military, what he observed while serving in law enforcement, and the changes he made, which are revealed in the chapter "When Blue Lines Become Grey." His narratives demonstrate why law enforcement personnel should not take shortcuts when going the extra yard is required.

Anecdotes from the author's career serve as a reminder that policing is dynamic, and no two situations will have the same outcome. "Stopping the Growing Trend" is a poignant chapter that applies to school safety officers and security professionals, who face the challenges of securing school environments against potential active shooter scenarios. Spencer's words are real and thought provoking.

This self-published book is written for those in law enforcement, and it applies to security professionals as well. While portions of the book offer advice on dealing with aspects of policing, the takeaway for the reader is that communication and respect go a long way in enhancing citizen interactions. It's sure to resonate with police officers and school safety officers.

REVIEWER: *Brian L. Royster, Ed.D., is an assistant professor at Saint Peter's University and a retired New Jersey State Trooper. He is a graduate of the FBI National Academy and a member of ASIS International.*



Everything you need to stay secure. G4S brings innovation to the forefront to help you leave risk behind. We can assess, equip, integrate and staff an end-to-end solution to secure your people, property and assets. It's physical security for your company and emotional peace of mind for your people, all created by the integration of our unique products. **To learn more about G4S Integrated Security Solutions, please visit www.g4s.us or email us at info@usa.g4s.com.**

Securing Your World

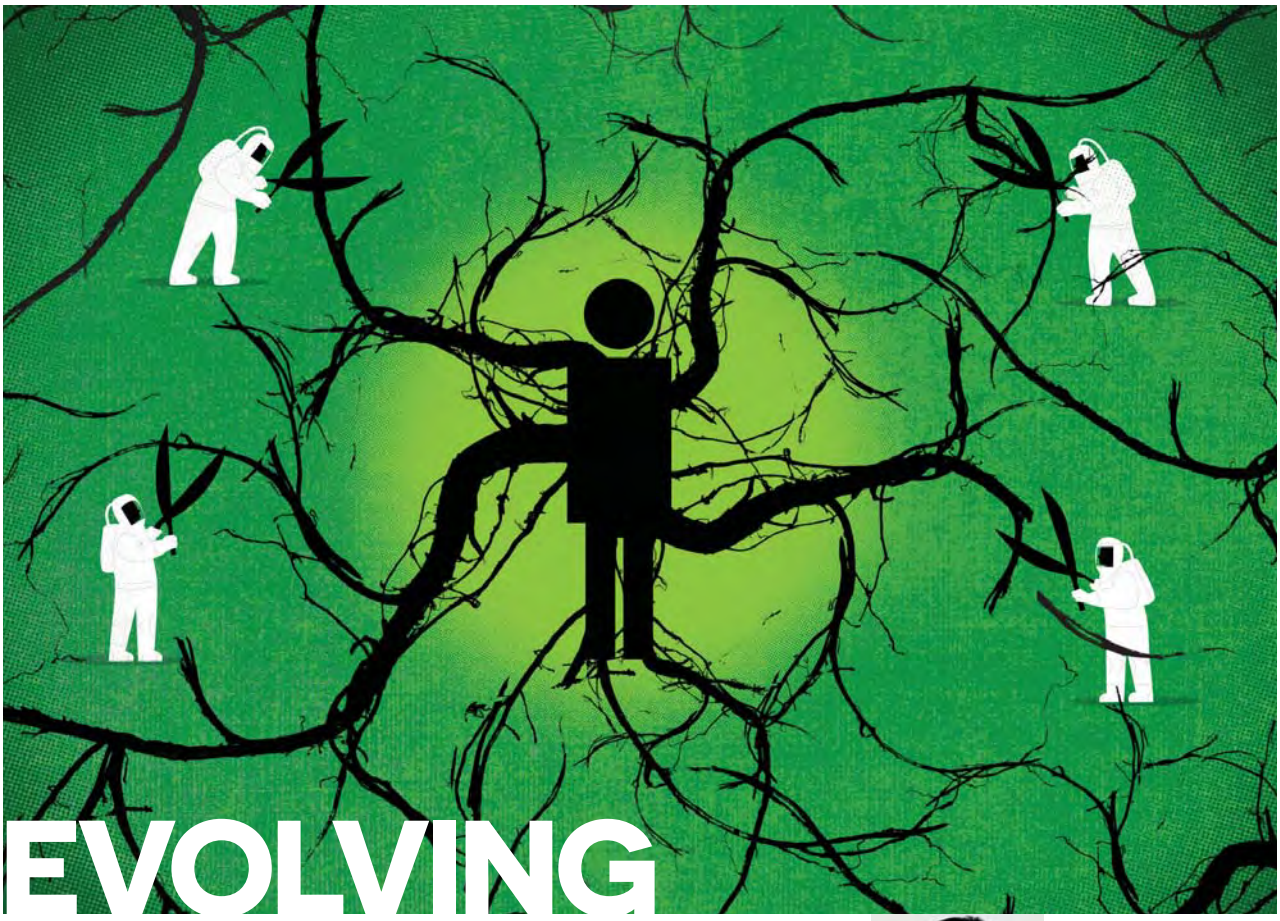


ILLUSTRATION BY MICHAEL AUSTIN

EVOLVING BIOTHREATS

DESPITE MULTIPLE CALLS FOR A UNITED APPROACH TO BIOLOGICAL THREATS, U.S. AGENCIES HAVE NO STANDARDIZED WAY TO SHARE THREAT AWARENESS OR ESTABLISH PLANS FOR DETECTION AND PREVENTION. **BY LILLY CHAPA**

CHIKUNGUNYA. ENTEROVIRUS. Cyclosporiasis. MERS. Ebola. Zika. Those are just a few of the outbreaks the United States has experienced over the past five years, according to the U.S. Centers for Disease Control and Prevention (CDC). And that doesn't include the dozens of foodborne outbreaks or diseases affecting pets and livestock that spread across the country each year.

These diseases not only take a toll on public health, the global food supply, and the agricultural sector, but they can be a threat to national security, according to the U.S. Government Accountability Office (GAO). Infectious diseases are spreading faster and emerging more rapidly than ever before, and nonstate actors continue to advocate for the use of biological weapons.

Despite being more than 15 years removed from the anthrax attacks that advanced the United States' biodefense posture, naturally occurring and manmade biological threats continue to pose a "catastrophic danger" to the country. But the national biodefense approach has not evolved with the emerging threats, according to a new GAO report.

"Biodefense is fragmented across the federal government, and we've reported in the past that there are more than two dozen presidentially appointed individuals with biodefense responsibilities," says Christopher Currie, director of emergency management, national preparedness, and critical infrastructure protection at GAO. Currie was the lead author of the recent GAO report, *Biodefense: Federal Efforts to Develop Biological Threat Awareness*.

GAO has reported on the agencies and programs that oversee the nation's biodefense for years, tracking programs such as BioWatch and laboratories containing hazardous pathogens. Currie acknowledges that the country's biodefense landscape is

complex due to the number of agencies involved and the breadth of threats.

"Each federal department has its own appropriations, own congressional oversight, and frankly its own world of stakeholders it deals with," he tells *Security Management*. "It's very difficult to make decisions across all of those on priorities when they are so separated. And everyone is involved to a different extent."

The lack of an overarching strategy makes it more difficult to get a well-rounded picture of emerging threats and how the agencies plan to respond.

The GAO report takes a detailed look at the role of each of the key biodefense agencies—the U.S. Departments of Homeland Security (DHS), Defense (DoD), Agriculture (USDA), Health and Human Services (HHS), and the Environmental Protection Agency (EPA)—and how they develop and report biological threat awareness.

"Part of the reason we did this was just to show and describe to people what is going on, because it's difficult to understand across all these agencies who does what and why," Currie says. "The goal of this was to get in there and understand behind the scenes what all the federal departments are doing to identify the risks and threats that would lead on to next steps of prevention and protection. That might inform what countermeasures you develop, what detection technologies you develop, and so on."

While each of the agencies plays an important role in managing biothreats in their sector, the lack of an overarching strategy makes it more difficult to get a well-rounded picture of emerging threats and how the agencies plan to respond.

"One of the things we talk about in this threat report is that clearly there's a lot of formal and informal coordinating and communication between these departments," Currie says. "The problem is, how does that translate into an overall prioritized strategy? That's where I think the efforts kind of stop, and it's vague what the government's overall strategy and goals are."

Currie points to the spread of Ebola to the United States in 2014 as illustrative of the lack of a united strategy. After a series of missteps at a Dallas hospital left one man dead of the disease and two nurses infected, the federal government called for procedural reviews and the CDC promised to deploy rapid response teams to future possible Ebola cases.

"You saw this with Ebola—the White House counsel tends to get very involved when these kinds of instances and crises happen. They immediately stand up these ad hoc groups to coordinate the response effort, but those quickly go away once the paranoia and panic dies down and we go back to the status quo," Currie explains. "That's a great example of why we're asking these questions about who's in charge. Is it CDC? DHS? The White House? Who's in charge of communicating to the public?"

GAO asked this question in a 2015 report on the fragmented biodefense enterprise, but not much has changed since then. The Blue Ribbon Study Panel on Biodefense, which is made up of former government officials and academic experts and analyzes the country's defense capabilities against biological threats, also came out with a 2015 report condemning the lack of federal leadership in the biodefense sector. The panel's primary recommendation

BOOK REVIEW

RESOLVING CONFLICTS

BY RICHARD E. RUBENSTEIN | Routledge; routledge.com; 160 pages; $44.95.

THE NEED for resolving conflicts is an issue that touches all aspects of modern society. When conflicts remain unresolved, anger and violence can ensue. International conflict can impact public policy, political rationale, and actions, and directly impact the citizenry.

In the book, *Resolving Structural Conflicts: How Violent Systems Can Be Transformed,* Richard Rubenstein offers an intellectual and academic approach to understanding the rationale for large conflicts. Rubenstein presents various aspects of the creation and potential resolution of conflict. The book includes detailed theoretical, historical, and political views pertaining to various aspects of conflict. These concepts include the potential causes of conflict based upon societal, religious, and geopolitical factors, the rationale for seeking resolution in a politically complicated environment, and the rationale for seeking resolution within complicated and turbulent settings. The content of the book is insightful yet broad enough to apply to various conceptual situations of cultural or political discord.

Although the book is well researched, supported, and composed, it will not assist industry professionals looking to deter acts of violence in the workplace. It does not offer methods or policies that can be easily applied to the business or corporate working environment. Better suited to those seeking a theoretical understanding of conflict, it would be useful for those working in governmental policy development or as a textbook in global politics and administration.

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

was for the U.S. president to appoint the vice president as the leader of federal biodefense efforts. "This is the single best action the Administration can take to resolve the continued challenges in biodefense," the panel states. "The ad hoc implementation of our other recommendations in the absence of this leadership will only result in more of the same uncoordinated effort."

The panel continues to call for implementation of its action items, noting the "limited progress" that has been made since the 2015 report. "The federal government could have—and should have—completed 46 of the action items

The 2017 National Defense Authorization Act requires the key agencies to develop a national biodefense strategy.

associated with our recommendations within one year," the panel states in a December 2016 assessment of federal efforts. "In the year since we published the Blueprint for Biodefense, the government made some progress on 17 of these, but only completed two."

Currie says he has not spoken directly with the current administration on whether it intends to make any changes in how biodefense is approached, but notes that the 2017 National Defense Authorization Act requires the key agencies to develop a national biodefense strategy. Currie says he's optimistic that the requirement will encourage the DoD, HHS, DHS, and USDA "to actually do what we've been saying for a few years now." The strategy was due to congressional committees in September 2017, but as of mid-November Currie says the process was still under way within the government. GAO will review the strategy once it is available and

determine whether it addresses shared threat awareness.

"I know they are working on it, clearly there is someone in the administration that's focused on it, but I don't know a lot about where this falls in terms of priority for this administration versus other threats like cybersecurity or countering violent extremism," Currie notes. "That's the part that is unknown."

Currie acknowledges that President Trump has proposed budget cuts within the different key agencies that may affect biodefense research and preparedness, but it is unclear whether Congress will approve those cuts. He points out that without an overarching strategy, it is more challenging to make sure the right agencies have the right funding.

"It does raise questions about how big a priority the biothreat part is for each of these agencies," Currie says. "What does the administration think about DHS's role in this versus what other agencies are doing? That's part of the problem with this, we really don't know how eliminating what one organization or department does will affect the entire enterprise because it's so fragmented."

Meanwhile, biological threats continue to spread, and there is no singular platform to track them all. The CDC and USDA websites each have different lists of foodborne outbreaks and recalls. The description of DHS's role in biological security is found under a "Preventing Terrorism" section and does not list any current threats or prevention activities. A search for DoD biological security efforts leads to an acronym-heavy webpage that was last updated in 2014. And, in other parts of the world, European Union member states are seeking funding to study the rapidly spreading African swine fever, which is infecting livestock, by declaring it a global health security threat.

"Ultimately, we've seen a lot of different strategies come out over the years about pieces of biodefense and surveillance," Currie says. "It's one thing to have a strategy, but you have to have the execution and implementation plan for the strategy. Departments have to be clear about what they are supposed to be doing, and there has to be some sort of accountability, and that's a big question: Who's going to be ultimately accountable and who are the departments going to answer to in actually implementing and executing the strategy? I'm hopeful that the strategy will address that issue, because without that it's going to be difficult across such a big enterprise to implement."

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

PHOTO COURTESY OF UNIVERSITY OF HAWAII AT HILO

FIND THE FIRE

THE UNIVERSITY OF HAWAII AT HILO UPGRADES ITS FIRE PANELS FOR INCREASED SPEED AND RELIABILITY. **BY HOLLY GILBERT STOWELL**

THE UNIVERSITY OF HAWAII AT HILO (UHH), founded in 1941, is located on the largest island of the Hawaiian archipelago, Hawaii–also known as "the Big Island." The school offers 38 undergraduate areas of study, including a renowned astronomy program, to approximately 3,600 students.

The Hawaiian skies over the central Pacific Ocean offer a spectacular view of the heavens.

But despite the campus's magnificent panoramas, the university's security staff found itself gazing too often at fire panels that weren't functioning properly, says Ted LeJeune, project manager at UHH.

When the campus began major renovations about five years ago, the security department ran into challenges with the fire panels, which worked via radio signal. "We were starting to experience issues with the reflectivity and the inconsistencies of the radio system," LeJeune says, "so we were having trouble passing our final fire inspections with the fire marshal."

The institution's fire system includes panels that intermittently report back to a central station in the campus security office. "On a regular basis, the panels transmit signals that say, 'Hey, I'm here, I'm doing fine,'" LeJeune explains. "And as long as we get that heartbeat notification, the security office knows that we don't have any problems."

The fire panels report any issues to the central station, including triggered smoke detectors, pulled fire alarms, and offline panels. When any of these alarms are triggered, "we get an immediate notification to our campus security office that we have an issue with a building, and we need to dispatch somebody to investigate," LeJeune notes.

In the campus security operations center, which is staffed around the clock, security staff members monitor a large screen that displays the fire life safety system's current status, as well as active alarms. The screen allows operators to scroll through notifications and keep an archive of reports. In case of fire or another life-threatening hazard, the fire department is contacted.

Let's Talk **Security**

Security Management editors and industry experts discuss topics that matter to you. Resubscribe to discover all that the new *Security Management* podcast has to offer.

Available on iTunes

SECURITY MANAGEMENT

STATS

Choosing a Fire and Life Safety System

What design factors are "extremely important" when selecting a fire and life safety system?

Product quality

70%

Service support

47%

Manufacturer's reputation

42%

SOURCE: *2016 FIRE AND LIFE SAFETY STUDY*, CONSULTING-SPECIFYING ENGINEER

The campus roofs are made of corrugated steel. But whenever the Hawaiian sun would hit the metal rooftops, the signals could get diffused or jammed, causing the radio-based fire alarm systems to report inconsistently, or not at all. This led to a host of issues for the campus security department.

"We were having intermittent connectivity and even losing connectivity to some of the locations because of the radio signal reflectivity of our roof systems," LeJeune says.

Besides the connectivity and transmission issues, the old radio units were burdensome to maintain, and an outside engineer had to travel to the campus to service the units.

These challenges led to a conversation with Digitize, which provides several aspects of the campus's fire life safety system. In the fall of 2016, Digitize suggested land-based radio units that connect into the university's existing fiber optic cable and Ethernet system. "We've done several upgrades over the last few years to standardize and stabilize our Internet," LeJeune explains, "and it was just a natural extension to add Digitize to the land system because we already had the existing backbone."

The land-based radio units allow the end user to remove the frequency transmitter on the fire panels, and connect into either the Ethernet or fiber connections in the buildings. This landline connection enables the panels to report back to the central station within seconds.

UHH launched a pilot project in the spring of 2017 to test the new product on its recently renovated College of Business

and Economics building. The university upgraded its base unit in the campus security office to accommodate both the radio frequency and the land inputs.

During the testing, the land-based units successfully and accurately reported all issues to the central station. "Our pilot project went fantastically," LeJeune says. "We were able to retrofit the remote unit [with the landline], and we were able to clearly communicate and program the base unit," he says. The school also brought the fire department in to observe the new system. "They were thrilled that we were getting a more stable network and that we were able to more clearly manage and supervise our system."

Since installing the new system, the campus has not experienced any issues with fire alarm panel reporting. Over the next several months, the campus plans to add additional land-based units to at least 25 buildings. Some of the larger buildings will have their own unit while groups of smaller buildings can share units, LeJeune adds.

"They were thrilled that we were getting a more stable network and that we were able to more clearly manage and supervise our system."

With the new system, UHH security staff can service the panels themselves, rather than relying on an outside engineer. "Digitize has given us in-house training, so that we can not only diagnose but also put new systems online, and program them at both ends to communicate consistently and properly," he notes. "The ability to work on them internally...and the training that we've been able to get from Digitize has just been a real major step forward for us."

He adds the new system allows security to fully focus on the issues that deserve attention. "It's about having confidence that we have consistent communications, and that we're not getting dropouts or false alarms," he says. "This allows the security office folks to focus on their assigned tasks rather than chasing ghosts and false alarms."

FOR MORE INFORMATION:

Abe Brecher, Digitize, www.digitize-inc.com, abeb@digitalize-inc.com, 973.219.2567

ILLUSTRATION BY STEVE McCRACKEN

GLOBAL CYBER AWARENESS

A GLOBAL SURVEY FINDS THAT MANY COMPANIES AT RISK OF CYBER-ATTACKS ARE UNPREPARED TO DEAL WITH THEM AND LACK AN OVERALL INFORMATION SECURITY STRATEGY. **BY MEGAN GATES**

ARBY'S. INTERCONTINENTAL HOTELS GROUP. Equifax. Deloitte. The U.S. Securities and Exchange Commission. Saks Fifth Avenue. UNC Health Care. Gmail. These are just a handful of the organizations that experienced a data breach in 2017.

But as these major cyber incidents grabbed international headlines week after week, were mulled over by regulators and legislatures across the globe, and spawned a slew of lawsuits, many organizations continued to struggle to comprehend and manage emerging cyber risks, according to PricewaterhouseCooper's (PwC's) recent report, *The Global State of Information Security Survey 2018 (GSISS)*.

The survey of more than 9,500 CEOs, CFOs, CIOs, CISOs, CSOs, vice presidents, and directors of IT and security practices from more than 122 countries found that the biggest potential consequences of a cyberattack were disruption of operations (40 percent), compromise of sensitive data (39 percent), harm to product quality (32 percent), physical property damage (29 percent), and harm to human life (22 percent).

"Yet despite this awareness, many companies at risk of cyberattacks remain unprepared to deal with them," the survey said. "Forty-four percent of the 9,500 executives in 122 countries surveyed by the 2018 *GSISS* say they do not have an overall information security strategy. Forty-eight percent say they do not have an employee security awareness training program, and 54 percent say they do not have an incident response process."

That's not to say, however, that executives assessed their preparedness uniformly across the globe. For instance, in Japan 72 percent of organizations said they had an overall cybersecurity strategy—possibly because cyberattacks are seen

Organizations that want to increase their resiliency will need to uncover and manage new risks in new technologies.

as the leading national security threat in the country.

But high preparedness does not translate into low risk for cyberattacks or incidents. The survey explained that while the United States is ranked second—behind Singapore—as the nation most committed to cybersecurity, it's still vulnerable to the number one business risk in North America: "large-scale cyberattacks or malware causing large economic damages, geopolitical tensions, or widespread loss of trust in the Internet."

The survey further explained that, based on U.S. Department of Homeland Security assessments, if more than 60 U.S. critical infrastructure entities were damaged by a single cyber incident, it "could reasonably result in $50 billion in economic damages, or 2,500 immediate deaths, or a severe degradation of U.S. national defense."

Because of this threat, PwC found that cyber resilient organizations will be those "best positioned to sustain operations, build trust with customers, and achieve high economic performance," according to the survey.

"Many organizations need to evaluate their digital risk and focus on building resilience for the inevitable," said Sean Joyce, PwC's U.S. cybersecurity and privacy leader, in the survey.

To achieve this level of resiliency, the survey results suggested seven initiatives: having leaders assume greater responsibility for building cyber resilience, digging deeper to uncover risks, engaging the board, pursuing resilience as a path to rewards, leveraging lessons learned, conducting stress-test interdependencies, and focusing on risks involving data manipulation and destruction.

Leadership. Most organizations' boards are not shaping their security strategies or investment plans—just 44 percent of *GSISS* respondents said that their corporate boards actively participate in their companies' overall security strategy.

"Senior leaders driving the business must take ownership of building cyber resilience," the report said. "Establishing a top-down strategy to manage cyber and privacy risks across the enterprise is essential. Resilience must be integrated into business operations."

The board and the CEO must drive this philosophy from the top down to accomplish this, says Ryan LaSalle, security growth and strategy lead at Accenture.

"If security is kind of an outsourced risk manager, where you throw risk over the wall and hope security catches it, it fails," he explains. "The only way security becomes more effective after all the innovation and investment's gone into it is if the business is accountable for it, and it's across the business."

Risks. Cybersecurity threats change daily, and organizations that want to increase their resiliency will need to uncover and manage new risks in new technologies. One of those risks includes those associated with the Internet of Things (IoT) ecosystem.

But few survey respondents said their organizations are planning to assess IoT risks. Respondents were also divided on who was responsible for assessing IoT risk in their organization: 29 percent said it belonged to the CISO, 20 percent said it belonged to the engineering staff, and 17 percent said it belonged to the chief risk officer.

"Many organizations could manage cyber risks more proactively," the

CYBERSECURITY LAW

BY TARI SCHREIDER. Rothstein Publishing; Rothstein.com; ebook; 233 pages; $14.74.

NOTED CYBERSECURITY lawyer Mark Rasch is credited with saying, "The rule is, 'if it moves, sue it...If it doesn't move, move it, then sue it.'" In today's litigious society, it's almost inevitable that a person or enterprise will be sued.

In *The Manager's Guide to Cybersecurity Law: Essentials for Today's Business*, author Tari Schreider provides a helpful resource that can help IT managers stay on the correct side of the myriad cybersecurity laws. While the author is not a lawyer, he does a good job in showing the reader what due diligence requirements must be taken to protect data under their control.

The book covers a lot in a little over 200 pages, including topics such as regulations, jurisdiction, U.S. laws addressing computer security, and digital forensics law. In addition to listing a number of high-profile cases and lessons that can be learned from them, it also includes several helpful checklists.

Each topic is covered in a few paragraphs, so this is certainly not a comprehensive guide. That said, it offers external links for further information. For those in IT looking for a quick and thorough introduction to cybersecurity law, this useful guide can help them comply with cybersecurity law rather than break it.

REVIEWER: *Ben Rothke, CISSP (Certified Information Systems Security Professional), PCI QSA (Qualified Security Assessor), is a principal eGRC consultant with the Nettitude Group.*

survey found. "Many key processes for uncovering cyber risks in business systems—including penetration tests, threat assessments, active monitoring of information security, and intelligence and vulnerability assessments—have been adopted by less than half of survey respondents."

One reason this might be the case is because many organizations are only addressing cybersecurity in a reactive manner, said Christopher Valentino, director of joint cyberspace programs and technical fellow at Northrop Grumman, in a presentation at CyberTalks in Washington, D.C.

Most cybersecurity technologies are all about reacting "to a breach, to a threat, to some event" based on something that we already know, such as a signature or pattern, Valentino explained. To be more resilient, organizations have to make a fundamental shift to being proactive in addressing cybersecurity threats.

All key industry sectors across the world would do well to stress-test their interdependencies with simulated cyberattack scenarios.

One way to do this is by training employees about cyberthreats through awareness campaigns and even spear phishing testing, Valentino said. Northrop Grumman does this, and Valentino, even with a vast background of cyber experience, said he failed his first test.

Companies also need to engage in better information sharing and coordination with stakeholders to address cyber risks, the PwC survey found.

"Only 58 percent of respondents say they formally collaborate with others in their industry, including competitors, to improve security and reduce the potential for future risks," the survey said. "Trusted, timely, actionable information about cyber threats is a critical enabler for rapid-response capabilities that support resilience. Across organizations, sectors, countries, and regions, building the capability to withstand cyber shocks is a team effort, the effectiveness of which will be diminished without greater and more significant participation."

Healthcare institutions, for instance, have been reluctant to share cyberthreat indicator information due to fears that regulators might come after them, said Christopher Wlaschin, CISO at the U.S. Department of Health and Human Services (HHS), at CyberTalks.

Some larger institutions that are sharing information are doing so through automated methods, but Wlaschin said most of the healthcare industry in the United States is not capable of machine speed sharing at this point because it lacks both the funding and the staff.

Because of this, HHS is working with Information Sharing and Analysis Centers (ISACs) to make shared information as meaningful as possible for those who choose to participate—especially in small, medium, and rural settings, Wlaschin explained.

The "collective awareness and preparedness of the healthcare sector relies on information sharing," he said.

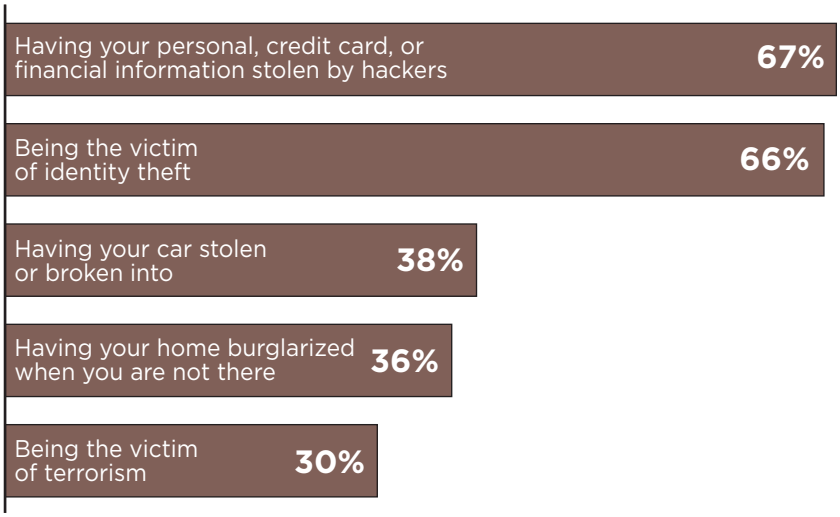
Lessons. Leaders from all sectors must work together to test cyber dependency and interconnectivity risks, and address accountability, liability, responsibility, consequence management, and norms, the PwC survey said.

To do this, the survey suggests that leaders take advantage of resources that offer insights into these issues, such as disaster response case studies, the National Association of Corporate

CYBERCRIME

Two-thirds of U.S. adults worry about becoming victims of cybercrime—far outweighing their concerns of more conventional crimes. A recent Gallup poll found a 28 percent gap between Americans' cybercrime fears and their next greatest concern: having their vehicle broken into.

Things Respondents Said They Worried About



SOURCE: *Cybercrime Tops Americans' Crime Worries*, Gallup, November 2017

Directors' *2017 Cyber Risk Oversight Handbook*, and emerging guidelines from the Information Sharing and Analysis Organization standards body.

The survey also recommends leaders look at emerging research to learn lessons on how to increase resiliency. For instance, the U.S. Department of Energy awarded $20 million to its National Laboratories and partners to develop cybersecurity tools to increase resilience and risk management of the U.S. electric grid and oil and gas infrastructure.

Testing. When patching a system, IT professionals typically engage in a testing period to make sure it works and to see what the patch's effect will be on the network. Industry sectors need to take the same approach to cybersecurity to boost resiliency.

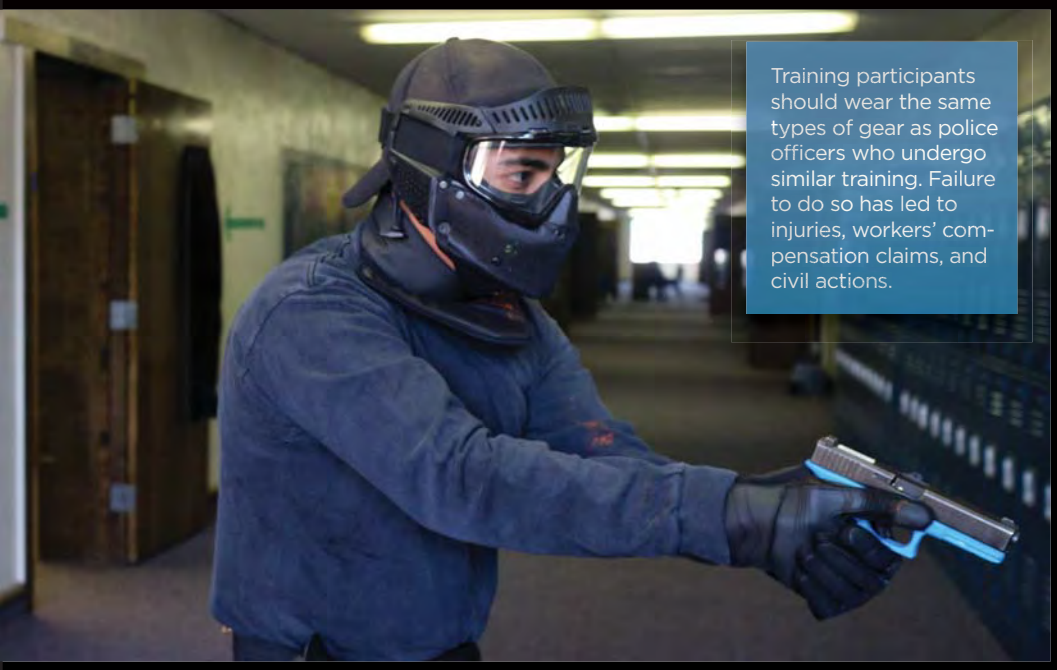
"All key industry sectors across the world would do well to stress-test their interdependencies with simulated cyberattack scenarios designed to inform risk management," PwC found. "Dan Geer, CISO at In-Q-Tel, has advocated developing cybersecurity stress test scenarios aimed at answering the following question: 'Can I withstand the failure of others on whom I depend?'"

Some sectors are already conducting these tests, such as the North American energy sector in its biennial GridEx exercise which simulates cyber and physical attacks on the electric grid, but more can be done to see how a widespread cyberattack would impact the sector—and others.

"Case studies of non-cyber disasters have shown that cascading events often begin with the loss of power—and many systems are impacted instantaneously or within one day, meaning there is generally precious little time to address the initial problem before it cascades," the survey said. "Interdependencies between critical and non-critical networks often go unnoticed until trouble strikes."

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

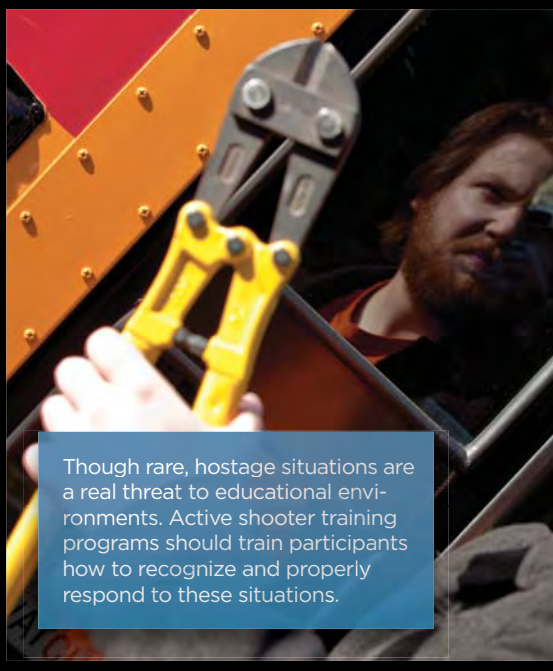
Put Training to



Training participants should wear the same types of gear as police officers who undergo similar training. Failure to do so has led to injuries, workers' compensation claims, and civil actions.

Training programs should avoid accidentally conditioning trainees that anyone with a gun is an active shooter.

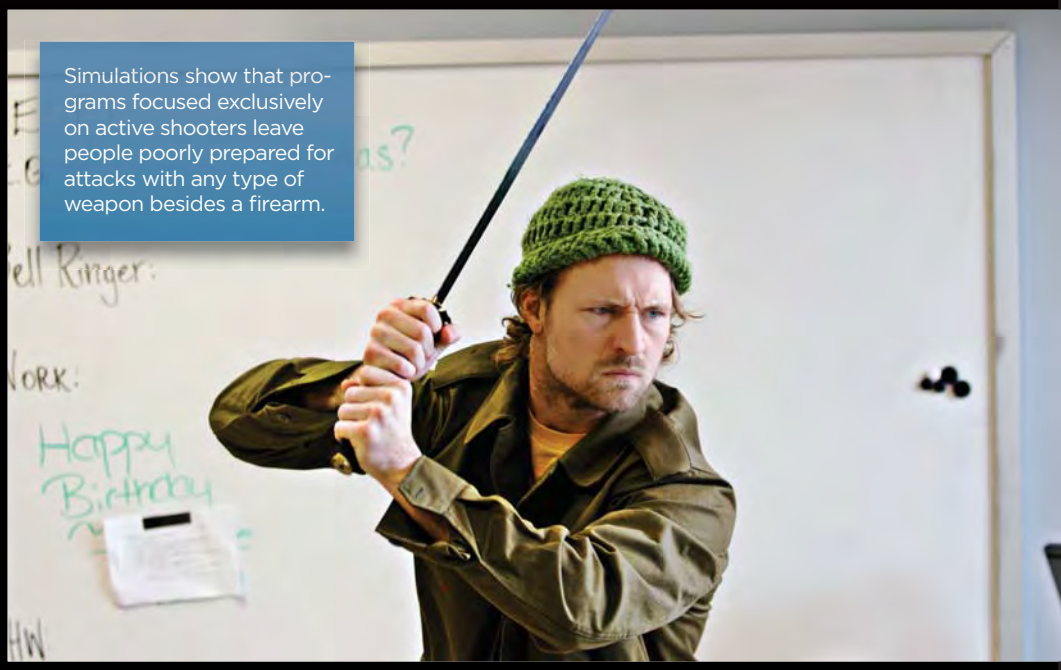
A high-quality active shooter training program will show participants how to respond to attacks involving weapons other than guns.



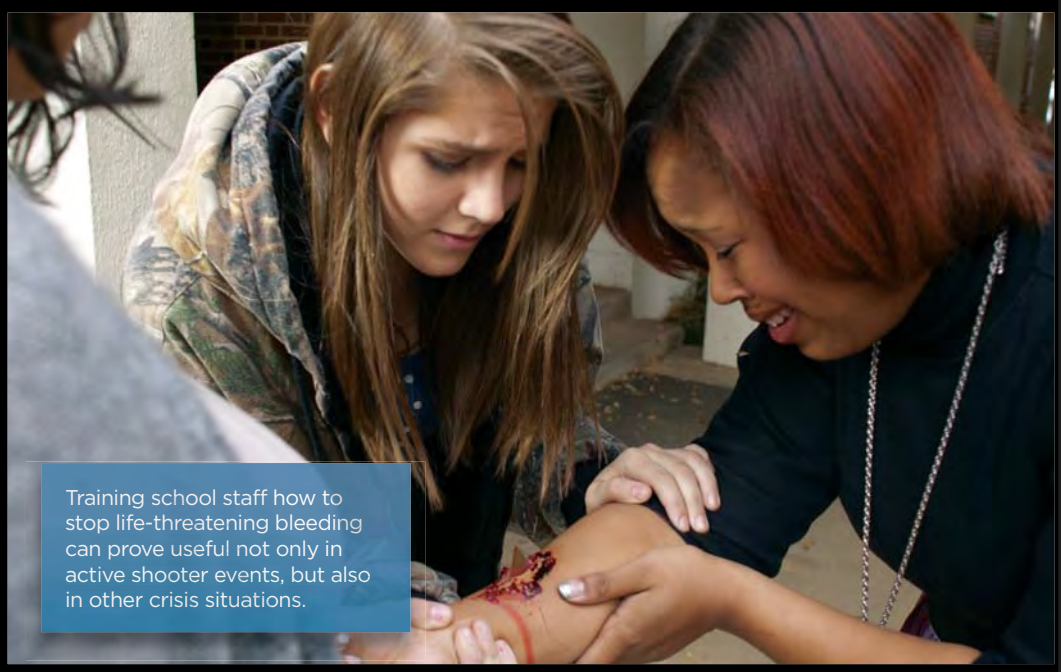
Though rare, hostage situations are a real threat to educational environments. Active shooter training programs should train participants how to recognize and properly respond to these situations.

the Test

By evaluating the effectiveness of scenario-based training, school administrators and faculty can learn to react appropriately to active threats, possibly circumventing tragedy.



Simulations show that programs focused exclusively on active shooters leave people poorly prepared for attacks with any type of weapon besides a firearm.



Training school staff how to stop life-threatening bleeding can prove useful not only in active shooter events, but also in other crisis situations.

PHOTOS BY RACHEL WILSON, SAFE HAVENS INTERNATIONAL

The classroom door flies open. An emotionally distraught student rushes into the doorway, produces a semiautomatic pistol, presses the muzzle of the gun to his temple with his finger on the trigger, and proclaims, "I can't take it anymore."

How will the teacher respond to this stressful, high-stakes situation? Will she intervene with verbal tactics or physical ones? Will she inadvertently put other students in danger by reacting too quickly?

An analysis by school security firm Safe Havens International found that teachers and administrators who had undergone traditional active shooter training were more likely to react to this situation by opting to attack the student or throw things at him, rather than taking the action steps outlined in the school's policies and procedures, such as calling 911 or instigating a lockdown. In other scenarios, trainees reacted in a similar manner that could intensify and aggravate the situation when time allowed for safer policies and procedures to be applied.

In the wake of high-profile massacres at schools and college campuses, institutions are preparing themselves for the emergency situations with scenario-based training programs.

The percentage of U.S. public schools that have drilled for an active shooter scenario rose from 47 to 70 percent from 2004 to 2014, according to a study by the National Center for Education Statistics. But the intensive search for solutions to these deadly events can lead to hasty planning and decision making, ultimately resulting in an ineffective response.

The number of teachers and administrators who opt to attack or otherwise approach the armed perpetrator indicates that current active shooter programs may be overwhelming for participants, causing them to respond to threatening scenarios in a dangerous way. Schools have also become narrowly focused on active shooter scenarios, when most deaths and accidents on campuses do not involve an active shooter.

Taking these factors into consideration, an all-hazards approach to scenario-based training allows schools to prepare for a range of incidents, including bullying, sexual harassment, and natural disasters. Fidelity testing then allows administrators and teachers to put those plans to the test and see how participants apply the training under stressful scenarios.

School leaders can then learn to rely on the solid foundational principles of policies and procedures, as well as communications and emergency plans, to diffuse potentially hazardous situations. Using these basic elements of active threat response and evaluating training programs to identify gaps could save lives.

Evaluations

During the stress of an actual crisis, people often react differently than they have been trained to do. Fidelity testing of a training program can help determine if there are gaps between what the trainer thinks the trainees will do, and what actions trainees will take in real life. This was the aim of evaluations completed by campus security nonprofit Safe Havens International of Macon, Georgia.

Methodology. Analysts conducted the evaluations at more than 1,000 K-12 public, faith-based, independent, and charter schools in 38 states. More than 7,000 one-on-one crisis scenario simulations were conducted by Safe Havens International in a series of school safety, security, and emergency preparedness assessments over the last five years. The participants were observed and scored by analysts who had completed a 16-hour formal training program and one day of field work.

Prior to running the scenarios, analysts came up with several action steps that should be taken in each scenario. These steps included initiating a lockdown, calling 911, sheltering in place, or pulling the fire alarm, for example. Based on those steps, the analysts developed a standardized scoring system to keep track of participant performance in the scenarios.

This type of training is known as options-based active shooter training because it gives the participants various responses to choose from. Many popular options-based programs are based on the U.S. Department of Homeland Security's Run. Hide. Fight. approach.

Drawing from Safe Havens International's repository of more than 200 audio and video crisis scenarios, analysts ran the simulations and let administrators, support staff, and teachers respond accordingly. These simulations covered a range of scenarios, which were presented in several formats.

For example, some participants were guided through an audio narration of a school bus taken hostage by an armed student. The audio was paused, and the trainees were asked what they would do next in that situation.

Similarly, video scenarios depicted potentially violent situations that left participants with a number of choices on how to react.

In one scenario, a woman screams at staff in the school office while brandishing a claw hammer. In another, a student on a school bus jumps up with a gun and yells, "Nobody move, and nobody gets hurt!" The video is stopped and trainees are prompted to say how they would react.

Based on action steps that were predetermined to be ideal, analysts then scored the trainees' responses on tablet devices. The scoring was be tailored to individual clients. For instance, if analysts were training a school district that has a police officer on every campus, its response would be different from that of a rural district that does not have a law enforcement officer within 20 miles.

Results. The results of the evaluations consistently showed that participants who were provided with options-based active shooter programs had lower scores than those who had not completed any type of training.

This outcome shows that current active shooter training methods may be overwhelming for administrators and teachers because they provide too much information—prompting them to attack when it is not necessary.

In an assessment in the northeastern United States, test subjects completed an options-based active shooter training program that was three and a half hours long. Evaluators found that the 63 administrators and staff members from 28 schools missed 628 out of 1,243 critical action steps that should have been implemented. That's more than 50 percent.

For example, participants failed to initiate or order a lockdown when it was appropriate 70 percent of the time. More than 55 percent of participants failed to call 911 or the school resource officer in scenarios depicting a person with a weapon, and 39 percent of participants failed to pull the fire alarm in situations involving fire.

Keeping Simulations Safe

EVEN THE MOST well-intentioned scenario-based training can result in injuries. Training programs that teach throwing of objects, taking people to the floor, punching and kicking, or similar uses of force can wind up hurting trainees and trainers alike.

PHOTO BY NATHAN JONES

At least one popular active shooter training program has resulted in high rates of serious injuries among trainees, according to Jerry D. Loghry, CPP, loss prevention information manager for EMC Insurance.

Loghry verified that EMC Insurance has paid out more than $1 million in medical bills to school employees for injuries sustained in trainings from one active shooter program over a 22-month time period. In addition, one police department is being sued due to those injuries.

Instructors can be trained on how to engage participants in use-of-force in a safe way. Reasonable safety measures should be put into place, such as floor mats, and participants should wear protective padding, goggles, and even helmets if necessary.

Safety rules should be written in advance and observed during training simulations.

Local law enforcement can be a valuable resource for simulating active threat situations in a safe manner, because police officers complete similar close-quarters combat training on a regular basis. Observing these best practices can help prevent litigation and liability issues, as well as enhance the overall experience of participants and instructors.

Current active shooter training methods may be overwhelming for administrators.

During an assessment of a school district in the southwestern United States, 32 people from two groups participated in scenario simulations. One group completed a five-hour live training program based on the Run. Hide. Fight. video, developed by the district's school resource officers. The second group did not receive the training or view the video.

The simulation results revealed that none of the top five scoring participants had received any type of active shooter training. All five of the lowest scoring participants, on the other hand, had completed the training program.

The overall score was also significantly lower for the group that had completed training than it was for the untrained group. The lower scoring participants often opted to attack in situations where it was not the best option.

Opting to attack. For the scenario described in the beginning of the article, where a student is potentially suicidal, analysts found that in one out of every four incidents, a school employee who had completed an options-based active shooter training would try to throw an object at or attack the student armed with a weapon.

Many of the participants in the simulations responded by opting to use force for almost any scenario involving a subject depicted with a gun. If the student in question was suicidal, such a reaction could be deadly, possibly leading to the student to shoot himself or others.

Participants who had not received formal training began talking to the student, encouraging him to put the gun down, and asking if it was okay for the other students in the classroom to leave. These basics of communication are essential in an active suicide threat situation and can help defuse possible violence.

Another scenario featured a drunk man who was 75 yards away from a school at the same time that a teacher and her students were 25 yards from the school building at recess. The analysis found that 30 percent of participants playing the teacher chose to approach—and even attack the drunk man—even though he was three-quarters of a football field away from the school.

The best option in this scenario is for the teacher to instruct the students to go into the school and put themselves in lockdown, then go into the building and ask the office to dial 911.

In November 2017, a school in Northern California initiated its lockdown procedure when the school secretary heard gunshots nearby. The gunman tried to enter the campus but could not find an open door. Because school faculty followed policies and procedures, countless lives were saved.

Fidelity Testing

FOR STEREO SYSTEMS, fidelity means that the sound generated by the speakers is nearly identical to the sound of the music that is recorded. In marriage, fidelity means that a person will be faithful to their promises to another.

In the world of school safety, fidelity indicates a close alignment between what is intended by safety policies, plans, drills, and training, and what people do in reality. Fidelity testing is the best way to verify the level of alignment between intentions and reality.

In the case of active shooter preparedness, fidelity testing involves efforts to measure whether there is a close match between theory and what people will actually do under the stress of a violent incident.

With properly designed active shooter preparedness approaches, practical application under extreme stress should mirror, to a reasonable extent, the theoretical expectations of the approach. If people cannot correctly apply the active shooter survival options they have been provided under simulated conditions, their performance will likely not improve when they are placed under extreme stress.

A high degree of fidelity helps reduce the distance between what people ideally do under stress and what they are likely to do. A

PHOTO BY RACHEL WILSON

reasonable level of fidelity testing of active shooter survival concepts should document that people are able to:

- Demonstrate the ability to identify when they are in an active shooter situation.
- Apply each option they are taught in an appropriate fashion when tested with scenarios they do not know in advance.
- Apply each option under limited time frames with incomplete information.
- Demonstrate knowledge of when applying each option would increase rather than decrease danger.
- Demonstrate the ability to identify when they are in a situation involving firearms that is not an active shooter event.
- Demonstrate the ability to properly address a wide array of scenarios involving weapons other than firearms.

Active Threat Approach

The narrow focus on active shooter incidents has left many schools ill-prepared for other active attacker methods, including edge weapons, acid attacks, and fire. Relying on active shooter training also neglects response to incidents that often go undetected, such as bullying and sexual harassment.

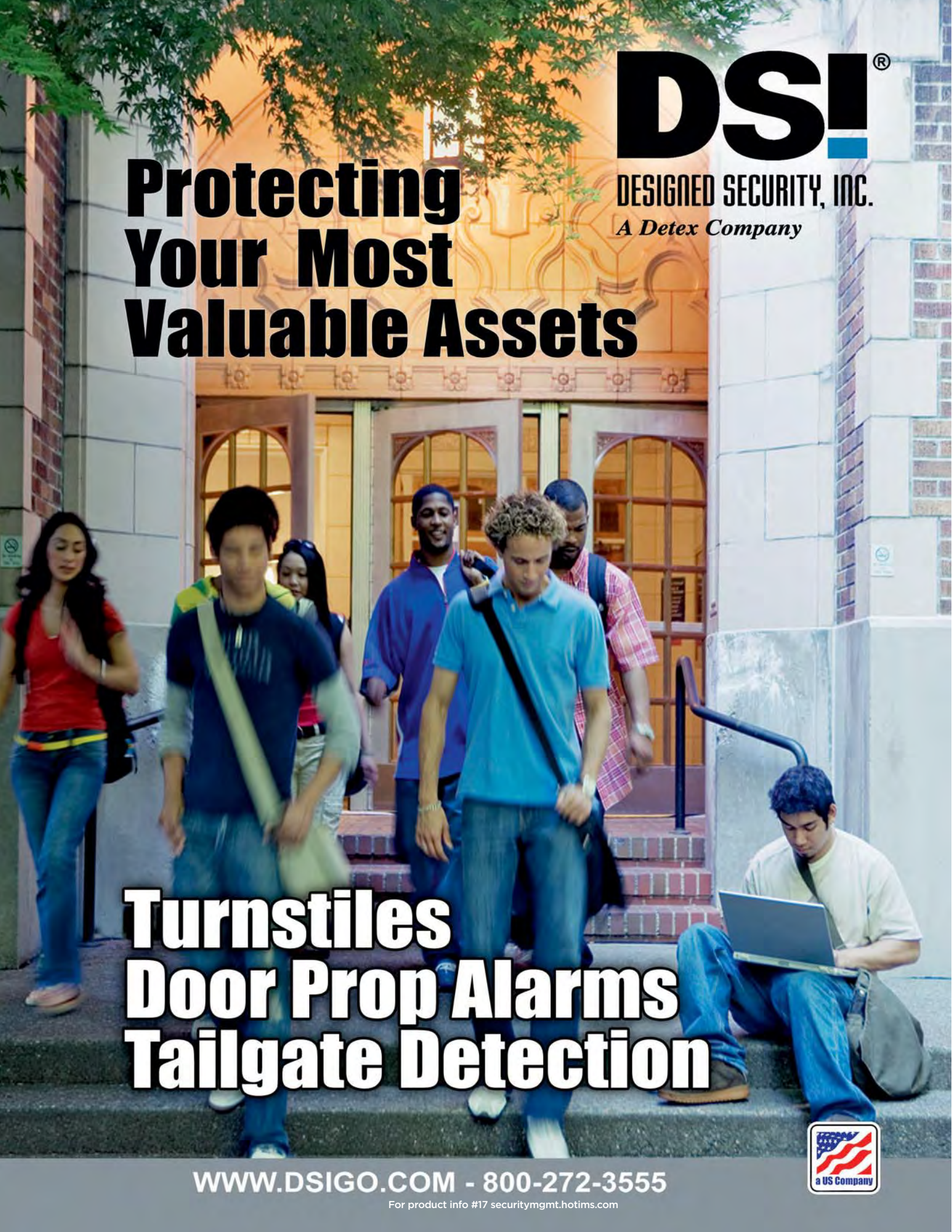
The Safe Havens International assessments revealed that many K-12 schools lack written protocols for hazardous materials incidents or do not conduct any training or drills for these easy-to-orchestrate, devastating types of attacks. Evaluations also revealed an unwillingness among some school staff to report incidents of sexual harassment.

Policies and procedures. Educational institutions have written policies and procedures on a range of issues, including bullying, sexual misconduct, signing in visitors, and traffic safety. Scenario-based training will help demonstrate whether staff are prepared to apply those policies appropriately. All staff should be included in this training, including bus drivers, cafeteria employees, and custodial workers.

Scenario-based training can reveal the gaps between what procedure dictates and what staff would actually do when confronted with a threat.

For example, in one simulation conducted by Safe Havens International, a student sat in a classroom with a teacher after hours. The teacher stroked the pupil's hair inappropriately and used sexually explicit language. Some custodial staff faced with this scenario responded that they did not feel comfortable reporting what they saw to school administrators. Janitors, who may be more likely to witness such incidents, said they felt an imbalance of power among the staff, leaving them unwilling to speak up.

Administrators should address such issues by using multiple scenarios related to sexual misconduct to demonstrate to



WWW.DSIGO.COM - 800-272-3555

For product info #17 securitymgmt.hotims.com

employees that they are not only empowered but required to report these situations. Reviewing these policies and procedures as part of scenario-based training, and incorporating possible threats other than active shooter, will bolster preparation among staff.

Attack methods. While mass shootings garner the most media attention, most recent homicides at schools were caused by attacks that did not involve active shooter events, according to *Relative Risk of Death on K12 Campuses* by school security expert Steven Satterly.

The 2014 study revealed that of 489 victims murdered on U.S. K-12 campuses from 1998 to 2013, only 62 were killed by active shooters. The Columbine, Sandy Hook, and Red Lake Reservation School shootings made up 74 percent of those 62 deaths.

Several weapons possibilities exist, and should be acknowledged in training programs, including edged weapons, explosive devices, and fire.

There have been dozens of mass casualty edged weapons attacks in schools, and serious damage can occur in a matter of minutes. A mass stabbing and slashing incident in Franklin, Pennsylvania, in April 2014 left 21 victims injured when a sophomore began attacking other students in a crowded hallway. Similar attacks have occurred in China, Japan, and Sweden that have killed and seriously injured students and school employees.

Acid attacks are occurring more frequently in the United Kingdom, as well as in India, East Africa, Vietnam, and other regions.

For example, in September 2016, a student rigged a peer's violin case with acid at a high school in Haddington, Scotland. The victim's legs were disfigured as a result.

Most recent homicides at schools did not involve active shooter events.

These types of attacks are relatively easy to carry out because acid is inexpensive and can be concealed in bottles that appear harmless. The injuries sustained in these attacks are gruesome and irreversible, and there are concerns that this attack method may become more common in the United States.

Many active shooter training approaches also fail to address combination attacks, in which the perpetrator uses two or more attack weapons, such as firearms and explosives, firearms and fire, and so forth.

In the 2013 attack at Arapahoe High School in Colorado, a student shot his classmates and a staff member several

times before throwing three Molotov cocktails that set part of the library ablaze. The student then shot himself.

Combination attack methods can present complications for first responders who may have to decipher where each threat is located and which one to deal with first. These campus attacks demonstrate the danger of training concepts that focus intently on active shooter incidents, while not offering viable options for other extreme attack methodologies.

There are ways to better prepare school staff to react to violence and reduce the chance of unintended consequences. Scenarios that present a range of threats and situations help trainees learn to react in the most effective manner, and remind them to rely on existing policies.

Fidelity testing that includes a scoring system for action steps will help determine whether active shooter and active threat training concepts have been received by the faculty. Including all staff members who have contact with students creates an inclusive environment where everyone feels empowered to report misconduct.

Putting a mirror to current school emergency preparedness will reflect where changes need to be made. If there are significant gaps between the training concept and application of those concepts when reacting unscripted to scenarios, improvements are in order. By applying these principles, schools can prepare themselves for the common emergencies, the worst-case-scenarios, and everything in between.

MICHAEL DORN IS THE CEO OF SAFE HAVENS INTERNATIONAL. HE HAS AUTHORED 27 BOOKS ON SCHOOL SAFETY AND EMERGENCY PREPAREDNESS, AND HIS WORK HAS TAKEN HIM TO 11 COUNTRIES. HE HAS PROVIDED POST-INCIDENT ASSISTANCE FOR 12 ACTIVE SHOOTER INCIDENTS AT K-12 SCHOOLS, AND HELPED COAUTHOR A U.S. GOVERNMENT IS360 WEB TRAINING PROGRAM ON ACTIVE SHOOTER EVENTS. HE CAN BE REACHED AT *MIKE@WEAKFISH.ORG*

Chase: Leading Through Change

Incoming ASIS President Richard Chase, CPP, PCI, PSP, spoke to *Security Management* about the state of ASIS—its current strengths, where it needs to evolve, and where it (and the security profession) will be going in the future.

Q. How did your career aspirations lead you to the security industry?

A. Post 9/11, I was asked by the U.S. Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), a law enforcement agency within the U.S. Department of Justice, to lead an effort to centralize the various security functions within the organization. At the time, these disciplines were spread throughout the different divisions with several of the programs requiring a more robust application. I came into this new role with more than 20 years of law enforcement experience and I thought I knew all there was to know about security management. A presumption that was quickly brought to rest!

To increase my knowledge base, I began to engage with other members of ASIS International to learn more about the private security sector and evaluate the efficacy of security systems and processes within the ATF. My experiences led to changes at the ATF. The agency's new headquarters building was the first to incorporate the new U.S. General Services Administration's security requirements resulting from the Oklahoma City Bombing. The ATF also adopted the new Chief Security Officer (CSO) construct within the executive management team.

Q. Why did you decide to volunteer some of your personal time to assist ASIS?

A. I wish I could say that I give back to the organization more than I receive, however that has not been my experience.

ASIS International has always been at the center of my individual development, as both a security practitioner and a manager. From the training seminars where I learned valuable information and met security professionals who were willing to share their experiences and best practices, to the rigorous preparation for the board certifications, this has always been true. All have profoundly influenced my ability to contribute to all aspects of my company's operations and, most importantly, the organization's overall growth and profitability.

Q. What are a few of ASIS's current strong points as a professional society?

A. The Society's greatest strengths continue to be the technical and geographical diversity of our membership and the "can do" attitude of our vast network of volunteer leaders.

Although ASIS represents a variety of different industries and countries, we still tend to speak the same security language while nurturing and

promoting the value of professional expertise. Our volunteer leaders throughout the world are second to none and represent a critical resource that has yet to be fully harnessed.

The annual seminar is also one of ASIS's great assets. Last year's event in Dallas was proof that participants will return home smarter, with a more substantial peer network and more exposure to the industry's most current product and service innovations. It will be the most important week of the security professional's year.

Q. How do you hope to see ASIS evolve in the next few years?

A. In an environment where the business topography is constantly changing, our success as an organization is directly aligned with our continuous ability to provide cutting-edge products and services that add a high value and a broad application to the membership.

As we all routinely experience in both our professional and personal lives, success is not something that just happens; it requires a plan and sound execution. Simply stated, my hope as we progress forward is that you will see a more agile and adaptable organization grounded by a strategic planning process—a process that fosters initiatives that are designed to identify the risks to our industry, assess their impact, contrast that to the cost of prevention, and then develop appropriate strategies for the future.

Fortunately, 2017 President Tom Langer, CPP, made that construct the centerpiece of his tenure on the Board. CEO Peter O'Neil, CAE, provided experience and leadership around staff implementation to support Tom's vision, so the Society is better positioned to identify and forecast the next opportunities on the horizon.

Those opportunities are already emerging, with the rebranding of our premier event, the Annual Seminar and Exhibits. For more than 60 years, ASIS has provided education, networking, and access to cutting-edge technologies through the seminar.

It is gratifying to see such a respected event move to the next level. So, I am particularly excited about changing the name of the Annual Seminar and Exhibits to the Global Security Exchange (GSX). The new name, and the continued changes to the event, reflect our organization's goal of advancing security worldwide and our commitment to grow and evolve with the security industry.

The newly rebranded GSX event in Las Vegas, Nevada, from September 23 to 27 will embody ASIS's commitment to bringing thousands of industry leaders from across the globe together for the most comprehensive security event in the world.

Q. ASIS currently has international members, but how can it grow into a truly global organization?

A. The Board and staff recognize that our prevailing operating model is obsolete and no longer aligns with the structural changes that have taken place in the global environment. Through O'Neil's leadership, much has been accomplished this past year in the area of organizational development in an effort to enhance the alignment of ASIS functions and services to meet the challenges of current and emerging membership markets.

Additionally, the findings and recommendations of an ad hoc working group, led by board member John Petruzzi, CPP, which focused on the expansion of the Society's international presence, have been incorporated into the latest ASIS International strategic plan.

Q. Will security managers of the future primarily be risk managers, business drivers, or something else?

A. The security professional of the future will be well versed in all of the above and then some!

Hopefully by now you have started to hear the buzz around enterprise security risk management (ESRM), a philosophy and practice that leverages a comprehensive management process to effectively address security risks across the enterprise.

By leveraging the expertise of our volunteer leaders, ASIS International is now strategically positioned to be at the forefront for the promulgation of ESRM training and guidelines. I would encourage the members to take advantage of the various ESRM training deliveries during the annual seminar and exhibits.

ASIS International and the cadre of volunteers continue to provide the framework for success—now and into the future. Take advantage of this great opportunity and get involved!

NEW TECHNOLOGY With a PERSONAL TOUCH

When Northwestern Mutual added a futuristic tower to its Milwaukee campus, it took its security approach to new heights.

As a financial services organization, Northwestern Mutual helps clients plan now to prepare for the future. And at the end of 2014, the Milwaukee-based company took that goal to task when planning a security strategy for a new building in the heart of the city. The 32-story, 1.1 million-square-foot Northwestern Mutual Tower and Commons houses about 2,400 Northwestern Mutual employees and signals a shift in the organization's approach to business.

"In essence, it was revolutionizing our organization from an insurance and financial investment company into a financial tech-savvy organization," explains Bret DuChateau, corporate security consultant at Northwestern Mutual. "How do we position ourselves over the next few years to build this brand new state-of-the-art building to attract the workforce of the future, and how leading up to that do we design and integrate systems into that building that will set us up for the future?"

DuChateau has been on Northwestern Mutual's security team since 2004, and the new building presented an opportunity to not only update the technology but position the organization's security approach as one that will be cutting-edge for years to come.

PHOTO COURTESY OF NORTHWESTERN MUTUAL

We had multiple campuses all under one corporate security team, but we were talking two different languages.

Key to this concept was considering how technology could augment a physical security presence through digital guest registration systems, data analytics, and streamlined command center protocols. First, however, DuChateau had to get the entire campus on the same security platform.

Come Together

"The tower is a learning center for all of our financial representatives and employees, designed in a very open and collaborative way from an organizational and customer experience standpoint," DuChateau says. "It certainly positions us where we want to be in the future, but is also designed to connect better with the community here in Milwaukee."

The new facility connects to three existing Northwestern Mutual buildings via skywalk and also boasts a public commons area featuring gardens, restaurants, and coffee shops, and an interactive museum of the organization's history. With the combination of old and new buildings, as well as public and private areas, it was critical for the campus's access control to work as a unified solution.

"We had multiple campuses all under one corporate security team, but we were talking two different languages," DuChateau explains. "You would have one system and one set of rules at one campus, and one system and set of rules at the other, and there was no data exchange, so you were always trying to manually keep databases in sync. If someone leaves one site, we have to manually take them out of the other site. Just onboarding and offboarding people, manually entering their first name, last name, and employee number in one system, assigning them access, and then turning to the next computer and entering them in another system. I could go on and on."

Northwestern Mutual chose AMAG Technology for its Symmetry access control enterprise system and Symmetry GUEST visitor management system to streamline the flow of employees and visitors alike throughout the campus. Now with all buildings on the same platform, and the ability to automate several of the processes that had previously been manual, Northwestern Mutual estimates it saves about 14 hours a month when it comes to managing the access control system.

"You're not only looking at a security process efficiency, but a support process," DuChateau explains. "Now we have dedicated IT teams that help us from an infrastructure standpoint—they don't have to remember which system they are working on, because we're all working on one system across the enterprise. We're in a virtualized server environment so everyone is seeing and touching the same thing, and just from a staffing standpoint, we have people who can bounce between multiple campuses and they are not having to relearn everything."

Comparing the response to a standard door alarm before and after the technology upgrade shows the efficiency of the new system, DuChateau points out. When multiple security systems were in place, a door alarm would be automatically logged into a database and a patrol officer would be dispatched to where the alarm went off. Employees in the command center would open up an Excel spreadsheet and document the date, time, and location of the alarm and how it was resolved. At the same time, the responding officer would record the same information into his or her own response log.

"We'd have this incident documented in five or six places," DuChateau notes. "In our traditional mindset a few years ago, we just kept doing it because it was the process. None of the documentation was coalesced into a common system, it was just out there."

After the AMAG upgrade, the process has become more streamlined. The access control system will register the door alarm and immediately display a notification on video monitors in the command center. The situation can often be resolved just by looking at the video of what is going on, and the system allows employees to document the alarm in the system itself.

"It's pretty hands-off, we put a heavy lift into the programming," DuChateau says. "We went from logging 1,400

different entries on a shift down to 200 just by taking a step back. When you're saving 800 steps from a shift, that equates to time, so we gained about six hours out of an eight-hour shift by freeing someone up from documenting everything."

Watchful and Welcoming

Northwestern Mutual's corporate security team is blended, with about 40 in-house employees and another 40 contracted officers. The organization switched from another contract security provider to G4S at the end of 2016 due to its familiarity with the AMAG systems—AMAG is a subsidiary of G4S.

"That was a factor in identifying this relationship," DuChateau says. "We could have the benefit of G4S folks coming to us that have familiarity with their own products already, so we don't have to spend as much time as we normally would with someone coming in cold and having to train them on the solutions."

DuChateau points out that, despite the addition of the tower and commons to the campus, Northwestern Mutual did not need to bring on any additional in-house or contracted security personnel, thanks to the augmented technology.

"When you talk about opening a 1.1 million-square-foot addition, you would think that it's a given that we'd need extra security people, but we didn't because we became more efficient," DuChateau says.

G4S officers have become a more integral part of Northwestern Mutual's security approach and are primarily in charge of the visitor management system, which is critical for the new facility—employees from all over the country flock to the Milwaukee campus every week for training. The increase in traffic required DuChateau to rethink the visitor registration process.

"We had five buildings that were all interconnected, but we had five separate lobbies, five separate ways to process visitors, five separate ways to get employees in and out, so we wanted to make some conscious decisions on where to direct people," DuChateau explains. "We just built this brand new beautiful tower and connecting commons and training space. Do we have to process visitors at every single building or can we direct them to the tower lobby? If we direct them to one main entry point, then we can deploy technology in these other lobbies and move resources where they're needed. We changed a little bit of behavior and moved some of the operations more towards a centralized location than doing everything everywhere."

AMAG's visitor management system allows guests to preregister, making it easy for officers to look up the guest and print a barcoded badge that permits visitors access to specified areas. The system also runs guests' names against a list of restricted visitors. DuChateau says that in the future the system will allow preregistered guests to print off a QR code that would produce a badge upon being scanned at the facility. "There are some cool things on the horizon as far as the efficiency standpoint goes," he says.

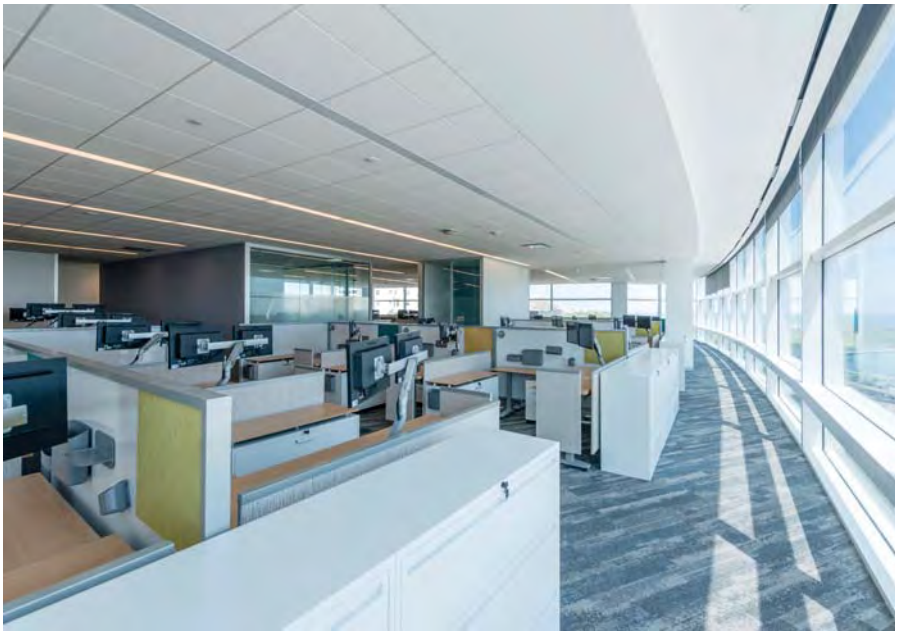
All in the Numbers

While DuChateau is glad to have a 21st century, enterprise-level security system in place, he says he is most looking forward to what the system can do for Northwestern Mutual in years to come. Already, data mining has made the security approach more efficient and intuitive.

"We have two cafeterias on our Milwaukee campus, so we can start gathering access control data and say at 9:30 a.m. here's a snapshot of the number of people on campus, give that to the restaurant team, and they can use it and plan to feed that many people for lunch that day," DuChateau says. "We want to use this data to say, 'okay, are we using our facilities how we had intended three years ago?' We start looking at singular systems, gathering data, and making that data actionable in a business sense. Data is data, but if you don't use it, what good is it for besides investigations?"

Preregistration data also helps the security team manage the flow of visitors each day. Employees can look at the guest database and estimate when and where large groups of visitors will arrive, and plan accordingly. "We get a couple more laptops, badge printers, and patrol people to help process visitors, versus having a bad customer experience and having 200 people lined up out the door just to get in to a training event that we're hosting," DuChateau explains.

Data is data, but if you don't use it, what good is it for besides investigations?



That's just the tip of the data-mining iceberg, and the more Northwestern Mutual's security arm works with the rest of the organization, the more the data can be employed to the organization's benefit. "Our information resource management and cybersecurity folks look at it from a different perspective, and maybe our privacy people ask how the data is going to be used and what kind of data is gathered," DuChateau says. "Now that we're standardized on an enterprise-class solution, how can that data benefit the business? How can we slice and dice that data down the road? Maybe we can take snapshots of our environment across all of our facilities, not only in Wisconsin but in Arizona and New York—can we feed that information to our workforce planning people?"

DuChateau says he wants Northwestern Mutual's intelligent security control centers to take the heavy lift off of employees and use built-in analytics to proactively identify strange behavior, and instead use security personnel to respond to exceptions.

"For the longest time, our control centers had this big screen up with all card access activity in the environment, thousands and thousands of people badging in and out—all of this data is scrolling by and it's just noise," DuChateau says. "Why do we even care what these people are doing in real time? Let's care about the people who are badging into areas that they aren't supposed to be badging into, or someone who has a multifactored device and is putting in the wrong PIN code, and start dealing with the smarter security approach to a secure environment."

We've really begun to scratch the surface on the potential of all of this technology.

While the new technology and data augment Northwestern Mutual's security posture and reduce the workload on guard services, DuChateau says that does not mean technology will replace people. "Maybe we want to pull some people because we've deployed technology, but we will direct them to a different part of the operation that looks at metrics, or quality assurance, or all of these things that really build up those parts of the program, because we don't have to be so labor intensive on physical access control or checking IDs or things like that—we can look at resource management in a different lens."

For now, DuChateau says the security team is still getting used to the new facilities and platforms at Northwestern Mutual's Milwaukee campus and is learning to rely on the data the systems collect. But within a few years, he foresees a "phenomenal expansion" of leveraging the platforms to guide the team's efforts.

"We've really begun to scratch the surface on the potential of all of this technology," DuChateau says. "We're in a good spot because we did it early enough and we have people familiar enough with the technology. Now we can ask, okay, what else can we do and how else can we move the vision of our company forward?"

CONTACT ASSOCIATE EDITOR **LILLY CHAPA** AT LILLY.CHAPA@ASISONLINE.ORG. FOLLOW HER ON TWITTER: @LILLYCHAPA.

ASIS EUROPE

ASIS EUROPE 2018

FROM RISK TO RESILIENCE

ROTTERDAM NETHERLANDS **18–20 APRIL 2018**

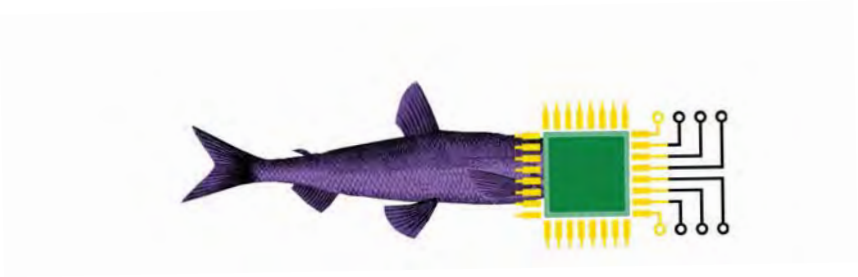
CYBER, PHYSICAL
OR INSIDER THREAT?

ALL OF THE ABOVE?

REGISTER BY 8 MARCH
FOR ADVANCE RATES

ASIS INTERNATIONAL
Advancing Security Worldwide®

www.asiseurope.org



HOW TO
Hack a Human

When cybersecurity measures become difficult to penetrate by technical means, people become the weakest link in the system.

It all started innocuously with a Facebook friend request from an attractive woman named Mia Ash. Once her request was accepted, she struck up a conversation about various topics and showed interest in her new friend's work as a cybersecurity expert at one of the world's largest accounting firms.

Then, one day Mia shared her dream—to start her own company. She had one problem, though; she did not have a website and did not know how to create one. Surely her new friend could use his expertise to help her achieve her dreams by helping her make one?

Mia said she could send him some text to include on the new site. He agreed, and when he received a file from Mia he opened it—on his work computer. That simple act launched a malware attack against his company resulting in a significant compromise of sensitive data.

ILLUSTRATION BY BORIS SÉMÉNIAKO

> **"Nobody had prepared him for a virtual honey trap, and he fell for the scheme without hesitation."**

Mia was not a real person, but a carefully crafted online persona created by a prolific group of Iranian hackers—known as Oilrig—to help this elaborate spear phishing operation succeed.

Due to his role in cybersecurity, the target was unlikely to have fallen for a standard phishing attack, or even a normal spear phishing operation. He was too well trained for that. But nobody had prepared him for a virtual honey trap, and he fell for the scheme without hesitation.

This case is a vivid reminder that when cybersecurity measures become difficult to penetrate by technical means, people become the weakest link in a cybersecurity system. It also illustrates how other intelligence tools can be employed to help facilitate cyber espionage.

While many hackers are merely looking to exploit whatever they can for monetary gain, those engaging in cyber espionage are different. They are often either working directly for a state or large nonstate actor, or as a mercenary contracted by such an actor tasked with obtaining specific information.

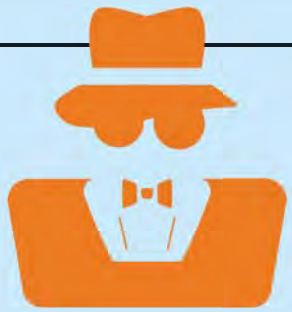
This targeted information typically pertains to traditional espionage objectives, such as weapons systems specifications or the personal information of government employees—like that uncovered in the U.S. Office of Personnel Management hack.

The information can also be used to further nondefense-related economic objectives, such as China's research and design 863 program, which was created to boost innovation in high-tech sectors in China.

Given this distinction and context, it is important to understand that hacking operations are just one of the intelligence tools sophisticated cyber espionage actors possess. Hacking can frequently work in conjunction with other intelligence tools to make them more efficient.

Hacking into the social media accounts or cell phone of a person targeted for a human intelligence recruitment operation can provide a goldmine of information that can greatly assist those determining the best way to approach the target.

For instance, hacking into a defense contractor's email account could provide important information about the date, time, and place for the testing of a revolutionary new technology. This information could help an intelligence



The **MICE** and **Men** Connection

The main espionage approaches that could be used to target an employee to provide information, network credentials, or to introduce malware can be explained using the KGB acronym of MICE.

M = Money. In many cases, this does equal cold, hard cash. But it can also include other gifts of financial value—travel, jewelry, vehicles, education, or jobs for family members. Historic examples of spies recruited using this hook include CIA officer Aldrich Ames and the Walker spy ring.

A recent example of a person recruited using this motivation was U.S. State Department employee Candace Claiborne, who the U.S. Department of Justice charged in March 2017 with receiving cash, electronics, and travel for herself from her Chinese Ministry of State Security handler, as well as free university education and housing for her son.

I = Ideology. This can include a person who has embraced an ideology such as communism, someone who rejects this ideology, or who otherwise opposes the actions and policies of his or her government.

Historical examples of this recruitment approach include the Cambridge five spy ring in the United Kingdom and the Rosenbergs, who stole nuclear weapons secrets for the Soviet Union while living in the United States.

agency focus its satellite imagery, electronic surveillance, and other collection systems on the test site.

Conversely, intelligence tools can also be used to enable hacking operations. Simply put, if a sophisticated cyber espionage actor wants access to the information contained on a computer system badly enough, and cannot get in using traditional hacking methods, he or she will use other tools to get access to the targeted system. A recent case in Massachusetts illustrates this principle.

Medrobotics CEO Samuel Straface was leaving his office at about 7:30 p.m. one evening when he noticed a man sitting in a conference room in the medical technology company's secure area, working on what appeared to be three laptop computers.

Straface did not recognize the man as an employee or contractor, so he asked him what he was doing. The man replied that he had come to the conference room for a meeting with the company's European sales director. Straface informed him that the sales director had been out of the country for three weeks.

The man then said he was supposed to be meeting with Medrobotics' head of intellectual property. But Straface told him the department head did not have a meeting scheduled for that time.

Finally, the man claimed that he was there to meet the CEO. Straface then identified himself and more strongly confronted the intruder, who said he was Dong Liu—a lawyer doing patent work for a Chinese law firm. Liu showed Straface a LinkedIn profile that listed him as a senior partner and patent attorney with the law firm of Boss & Young.

Straface then called the police, who arrested Liu for trespassing and referred the case to the FBI. The Bureau then filed a criminal complaint in the U.S. District Court for the District of Massachusetts, charging Liu with one count of attempted theft of trade secrets and one count of attempted access to a computer without authorization. After his initial court appearance, Liu was ordered held pending trial.

Straface caught Liu while he was presumably attempting to hack into the company's Wi-Fi network. The password to the firm's guest network was posted on the wall in the conference room, and it is unclear how well it was isolated from the company's secure network. It was also unknown whether malware planted on the guest network could have affected the rest of the company's information technology infrastructure.

The fact that the Chinese dispatched Liu from Canada to Massachusetts to conduct a black bag job—an age-old intelligence tactic to covertly gain access to a facility—indicates that it had not been able to obtain the information it desired remotely.

China had clear interest in Medrobotics' proprietary information. Straface

---

One recent example of an ideologically motivated spy is Ana Montes, who was a senior U.S. Defense Intelligence Agency analyst recruited by the Cuban DGI, who appealed to her Puerto Rican heritage and U.S. policies toward Puerto Rico. Another ideologically motivated spy was Chelsea Manning, a U.S. Army private who stole thousands of classified documents and provided them to WikiLeaks.

C = Compromise. This can include a wide range of activities that can provide leverage over a person, such as affairs and other sexual indiscretions, black market currency transactions, and other illegal activity. It can also include other leverage that a government can use to place pressure on family members, like imprisoning them or threatening their livelihood.

Historic examples of this approach include U.S. Marine security guard Clayton Lonetree, who was snared by a Soviet sexual blackmail scheme—a honey trap—in Moscow, and FBI Special Agent James Smith who was compromised by a Chinese honey trap.

More recently, a Japanese foreign ministry communications officer hung himself in May 2004 after falling into a Chinese honey trap in Shanghai.

E = Ego. This approach often involves people who are disenchanted after being passed over for a promotion or choice assignment, those who believe they are smarter than everyone else and can get away with the crime, as well as those who do it for excitement.

Often, ego approaches involve one of the other elements, such as ego and money—"I deserve more money"—or ego and compromise—"I deserve a more attractive lover."

A recent example is the case of Boeing satellite engineer Gregory Justice, who passed stolen electronic files to an undercover FBI agent he believed was a Russian intelligence officer. While Justice took small sums of money for the information, he was primarily motivated by the excitement of being a spy like one of those in the television series *The Americans*, of which he was a fan.

told FBI agents that companies from China had been attempting to develop a relationship with the company for about 10 years, according to the FBI affidavit. Straface said he had met with Chinese individuals on about six occasions, but ultimately had no interest in pursuing business with the Chinese.

Straface also noted that he had always met these individuals in Boston, and had never invited them to his company's headquarters in Raynham, Massachusetts. This decision shows that Straface was aware of Chinese interest in his company's intellectual property and the intent to purloin it. It also shows that he consciously attempted to limit the risk by keeping the individuals away from his facilities. Yet, despite this, they still managed to come to the headquarters.

Black bag attacks are not the only traditional espionage tool that can be employed to help facilitate a cyberattack. Human intelligence approaches can also be used.

> "Other intelligence tools can be employed to help facilitate cyber espionage."

In traditional espionage operations, hostile intelligence agencies have always targeted code clerks and others with access to communications systems.

Computer hackers have also targeted humans. Since the dawn of their craft, social engineering—a form of human intelligence—has been widely employed by hackers, such as the Mia Ash virtual honey trap that was part of an elaborate and extended social engineering operation.

But not all honey traps are virtual. If a sophisticated actor wants access to a system badly enough, he can easily employ a physical honey trap—a very effective way to target members of an IT department to get information from a company's computer system. This is because many of the lowest paid employees at companies—the entry level IT staff—are given access to the company's most valuable information with few internal controls in place to ensure they don't misuse their privileges.

Using the human intelligence approaches of MICE (money, ideology, compromise, or ego), it would be easy to recruit a member of most IT departments to serve as a spy inside the corporation. Such an agent could be a one-time mass downloader, like Chelsea Manning or Edward Snowden.

Or the agent could stay in place to serve as an advanced, persistent, internal threat. Most case officers prefer to have an agent who stays in place and provides information during a prolonged period of time, rather than a one-time event.

IT department personnel are not the only ones susceptible to such recruitment. There are a variety of ways a witting insider could help inject malware into a corporate system, while maintaining plausible deniability. Virtually any employee could be paid to provide his or her user ID and password, or to intentionally click on a phishing link or open a document that will launch malware into the corporate system.

An insider could also serve as a spotter agent within the company, pointing out potential targets for recruitment by directing his or her handler to employees with marital or financial issues, or an employee who is angry about being passed over for a promotion or choice assignment.

An inside source could also be valuable in helping design tailored phishing attacks. For instance, knowing that Bob sends Janet a spreadsheet with production data every day, and using past examples of those emails to know how Bob addresses her, would help a hacker fabricate a convincing phishing email.

Insider threats are not limited only to the recruitment of current employees. There have been many examples of the Chinese and Russians recruiting young college students and directing them to apply for jobs at companies or research institutions in which they have an interest.

In 2014, for instance, the FBI released a 28-minute video about Glenn Duffie Shriver—an American student in Shanghai who was paid by Chinese intelligence officers and convicted of trying to acquire U.S. defense secrets. The video was designed to warn U.S. students studying abroad about efforts to recruit them for espionage efforts.

Because of the common emphasis on the cyber aspect of cyber espionage—and the almost total disregard for the role of other espionage tools in facilitating cyberattacks—cyber espionage is often considered to be an information security problem that only technical personnel can address.

But in the true sense of the term, cyber espionage is a much broader threat that can emanate from many different sources. Therefore, the problem must be addressed in a holistic manner.

Chief information security officers need to work hand-in-glove with chief security officers, human resources, legal counsel, and others if they hope to protect the companies and departments in their charge.

When confronted by the threat of sophisticated cyber espionage actors who have a wide variety of tools at their disposal, employees must become a crucial part of their employers' defenses as well.

Many companies provide cybersecurity training that includes warnings about hacking methods, like phishing and social engineering, but very few provide training on how to spot traditional espionage threats and tactics. This frequently leaves most workers ill prepared to guard themselves against such methods.

Ultimately, thwarting a sophisticated enemy equipped with a wide array of espionage tools will be possible only with a better informed and more coordinated effort on the part of the entire company.

SCOTT STEWART IS VICE PRESIDENT OF TACTICAL ANALYSIS AT STRATFOR.COM AND LEAD ANALYST FOR STRATFOR THREAT LENS, A PRODUCT THAT HELPS CORPORATE SECURITY PROFESSIONALS IDENTIFY, MEASURE, AND MITIGATE RISKS THAT EMERGING THREATS POSE TO THEIR PEOPLE, ASSETS, AND INTERESTS AROUND THE GLOBE.

At ASIS 2017, attendees, including Alex Roark, took a deep dive into ESRM through an interactive exercise.

SHIFTING INTO HIGH GEAR

ENTERPRISE SECURITY RISK MANAGEMENT (ESRM) activity at ASIS is moving into high gear. The ASIS Board of Directors approved a plan for ESRM principles to be infused into the DNA of the Society. Designating ESRM a priority strategic initiative, the ASIS Board created the ESRM Commission in July 2016. In the year plus since, the commission inventoried ESRM content, identified subject matter experts, developed a primer, and interviewed members on how ESRM should be worked into ASIS's activities.

For the first time, in 2017, the ASIS Annual Seminar & Exhibits featured a full track of sessions devoted to ESRM. Sessions included a preseminar program on IT security for physical security professionals and an intensive interactive two-hour tabletop exercise in which attendees represented various departments of an organization and used ESRM principles to deal with an evolving crisis scenario. Earlier in the year, ASIS Europe 2017 focused on enterprise-level risks and featured master classes on implementing integrated enterprisewide security teams.

On November 15, the board approved the commission's request to transform into four workstreams that will develop appropriate ESRM material for their particular areas. The workstreams cover standards and guidelines, education and certification, marketing and branding, and creation of a digital maturity model tool. Each workstream includes a board member sponsor, an ASIS staff member, an ESRM subject matter expert, and a team of member volunteers.

Are you an avid ESRM advocate? Have you put ESRM into practice? There's still room in the workstreams for your expertise. Please contact Chief Global Knowledge and Learning Officer Michael Gips at *michael.gips@asisonline.org*.

ADAMS TO LEAD 2018 PROFESSIONAL CERTIFICATION BOARD

The ASIS Professional Certification Board (PCB) will be led in 2018 by Dana Adams, CPP, director of corporate security for TELUS, a telecommunications company headquartered in Vancouver, Canada. Adams has served on the PCB for six years and was the board's vice president in 2017. William Moisant, CPP, PSP, will assume the role of vice president in 2018.


Adams

The PCB oversees the ASIS board certification program and ensures that the domains of knowledge and the exams reflect the duties and responsibilities of security professionals. Adams succeeds 2017 President Per Lundkvist, CPP, PCI, PSP.

"I would like to thank Per for his able leadership of the PCB, as well as

ASIS Middle East 2017 took place in Bahrain in early November. More than 600 attendees learned about a broad range of key topics, visited cutting-edge exhibits, and networked with global security leaders.

for his guidance, support, confidence, and friendship," Adams says. "In 2018, priorities include continuing the work to establish an entry-level certification, maintaining the leadership role of ASIS board certifications across our profession, and ensuring global representation and diversity of the PCB."

New to the PCB in 2018 are Kevin Peterson, CPP, president, Innovative Protection Solutions, LLC; Jeffrey Leonard, CPP, PSP, area vice president, Securitas Critical Infrastructure Services, Inc.; and Vasiles Kiosses, CPP, PSP, physical security services manager, Schlumberger Oilfield Services. ASIS extends its thanks to departing PCB members, James Bradley, CPP, PCI, and Ann Trinca, CPP, PCI, PSP.

ASIS EUROPE 2018: FROM RISK TO RESILIENCE

Now is the time to register for ASIS Europe 2018, taking place 18-20 April in Rotterdam, The Netherlands. The event focuses on securing organizations in the era of IoT and highlights how enterprise security risk management approaches can protect an organization's full range of physical, digital, and human assets.

The "From Risk to Resilience" event format, launched in Milan in March 2017, will be repeated, with its mix of conference, training, technology and solutions, exhibition, career center, and exclusive networking.

At the conference, themed "Blurred Boundaries—Clear Risks," attendees will tackle the impacts of Big Data and artificial intelligence, and examine up-to-date risk outlooks, case studies, and analysis across the full range of key security management issues.

ASIS Europe will help attendees navigate a broad sweep of risks, from the malicious use of the latest emerging technologies to the threat of low-tech attacks, particularly on soft targets in public spaces.

Conference highlights include:

- Opening keynote on Big Data, automation, and artificial intelligence

ASIS BOARD OF DIRECTORS

PRESIDENT
- Richard E. Chase, CPP, PCI, PSP
  General Atomics
  San Diego, California

PRESIDENT-ELECT
- Christina Duffey, CPP
  SOS Security LLC
  Phoenix, Arizona

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

SECRETARY
- John A. Petruzzi, Jr., CPP
  G4S North America
  New York, New York

CHAIRMAN OF THE BOARD
- Thomas J. Langer, CPP
  BAE Systems Inc.
  Arlington, Virginia

DIRECTORS
- Charles E. Andrews, CPP
  Friends of Chuck
  Houston, Texas
- Howard J. Belfor, CPP
  Belfor & Associates
  Black Mountain, North Carolina
- Michael R. Bouchard, CPP
  Janus Global Operations
  Reston, Virginia
- Gail Essen, CPP, PSP
  Professional Security Advisors
  Andover, Minnesota
- Radek Havlis, CPP
  PricewaterhouseCoopers
  Prague, Czech Republic
- Jeffrey J. Lee, CPP
  Saudi Aramco
  Dhahran, Saudi Arabia
- Richard F. Lisko, CPP
  Willis Towers Watson
  Dallas, Texas
- Timothy M. McCreight, CPP
  Hitachi Systems Security
  Calgary, Alberta, Canada
- Darren T. Nielsen, CPP, PCI, PSP
  WECC
  Peoria, Arizona
- Jaime P. Owens, CPP
  Panama Canal Authority
  Panama City, Panama
- Malcolm C. Smith, CPP
  Qatar Museums
  Doha, Qatar
- Ann Y. Trinca, CPP, PCI, PSP
  SecTek
  Reston, Virginia

from a business perspective
- Digital asset valuation and risk assessments by Carl Erickson, CPP, and Gal Messinger of Philips Lighting
- The EU General Data Protection Regulation (GDPR) by Axel Petri of Deutsche Telekom and Christoph Rojahn of PricewaterhouseCoopers
- Jihadi terrorism trends in Europe by Glenn Schoen of *Boardroom@Crisis*
- Virtual security operation center transformation by Michael Foynes of Microsoft
- Public spaces as the front line against extremist violence by Thomas Vonier, CPP, of the American Institute of Architects
- Understanding business resilience by Laura Poderys of Danske Bank


© CARL BOWER
Vonier


Poderys

The conference is geared towards professionals who need to understand the full spectrum of physical and cyberthreats. Both established and aspiring security leaders can create learning paths through the program.

Register at *www.asiseurope.org*. Advance rates are available until March 8, and group packages are also available. Contact *europe@asisonline.org* directly for more information.

NEW ASIS WEBSITE, COMMUNITY

Digital transformation is at the forefront of many organizational discussions, and the need for innovation has never been greater. Remaining relevant in today's on-demand, content-driven world means that associations must be hyper-connected and agile.

With a clear directive to transform the organization through the strategic use of technology, ASIS is currently engaged in a broad range of innovative projects—including a major redesign of its primary website, *www.asisonline.org*, and the underlying technologies that support online and mobile experiences.

This month, ASIS launches Phase One of a multiyear project focused on improved and personalized content access, user-centric search and commerce, online community, and integrated systems for learning and certification.

One of the key strategies driving the new site is to create a powerful search function that will unify content from a

ASIS CLASSROOM PROGRAMS

MARCH

12–13 CPP, PSP Review, Orlando, Florida, USA

12–15 ASIS Assets Protection Course: Principles of Security (APC I), Orlando, Florida, USA

ASIS GLOBAL EVENTS

APRIL

16-17 ASIS NYC Security Conference and Expo, New York City, New York, USA

18–20 ASIS Europe, Rotterdam, The Netherlands

ASIS WEBINARS

JANUARY

10 Physical and Cyber Security: A Synergistic Relationship

31 Turning the EU General Data Protection Regulation (GDPR) into a Business Asset

FEBRUARY

7 Organized Crime as a Cyber Threat

21 Implicit Bias and Security Professionals

View the full education lineup at *asisonline.org/learn*

#MYASIS IMAGE OF THE MONTH

MYASIS-INTL on **TWITTER**

RT ASIS Security: What a great @ASISSecurity @ASIS_Intl Professional Educational SFM Seminar and Field Trip at the @WWIImuseum with our gracious Hosts Today.

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***.

ASIS INTERNATIONAL
Advancing Security Worldwide®

SECURITY MANAGEMENT

variety of ASIS sources, including *Security Management* offerings and Seminar sessions. By creating a search-centric site that allows users to filter results, ASIS will meet its goal of helping members at their "moment of need." The website facelift includes a more graphical and modern interface for both desktop and mobile devices.

It is important to understand that this is just Phase One of the process. With a critical emphasis on design, taxonomy, search, and commerce, both functionality and content are priorities. Additionally, some functionality will be moving to other platforms, such as the new community site, launching in February. Two other phases are planned for 2018.

ASIS is also upgrading the membership database, including new functionality for engagement, certification, profile management, and data analytics. The system will be tightly integrated with the website to ensure a seamless user experience across platforms. As a part of the new launch, ASIS will be engaging members to fully update their online profiles, both to help drive online personalization and to comply with the EU General Data Protection Regulation in 2018.

When the online community is launched, ASIS will provide security professionals with a secure platform to network, share ideas, access resources, and stay connected with peers, chapters, ASIS staff, and industry thought leaders.

Get ready, the launch of a new digital ASIS will be here soon!

Note: The ASIS website may be inaccessible for a few days at the end of January to facilitate the launch.

By Peggy O'Connor, ASIS director of communications. Contact her at peggy.oconnor@asisonline.org. Follow her on Twitter @pegoco.

MEMBER BOOK REVIEW

The Manager's Handbook for Corporate Security, Second Edition. **By Edward P. Halibozek and Gerald L. Kovacich.** Butterworth-Heinemann; Elsevier.com; 498 pages; $120.

Whether the reader is an aspiring security management student or a

CERTIFICATION PROFILE

DARIN DILLON, CPP

He admits that he got into the security field by mistake. Thirty-five years ago, Darin Dillon, CPP, replied to a classified ad in his local newspaper and landed a job as an installation and service specialist with Rollins Protective Services. That position became the basis of his employment master plan. "I have found security to be the coolest and greatest industry on the planet," he says.

Today, Dillon is business development manager with Convergint Technologies, a position he has held for the past 13 years. He looks forward to the moments when he can "solve a problem, meet a new person, share a new concept, or help someone in this exciting industry."

Dillon focuses on developing business and implementing complex electronic security for Fortune 1000 companies, hospitals, universities, and government municipalities. Because his position has a variety of responsibilities, "each day is a surprise," he says.

After arriving at his Houston, Texas, office each morning, Dillon sorts through his emails, texts, and voicemails and reacts accordingly to changes in his projects' priorities. But his most important responsibility? "It's my job to provide unparalleled customer service to those who count on our team for their global electronic security needs."

His quest to be viewed as a valued partner by these customers led Dillon to pursue the Certified Protection Professional® (CPP) designation in 2002. "Many of my clients had attained their CPP certifications, and I wanted to be tested to the same proficiency level they possessed," he says.

Dillon cites three factors that motivated him to study for the test over two years: "I wanted to know what my clients knew, I wanted to prove that I was in this industry for the long haul, and I wanted to stand out among my peers." His perseverance paid off when he received a passing score. Looking back, he says, this accomplishment catapulted him to where he is today.

A member of ASIS International for more than 25 years, Dillon has taken advantage of the educational and networking opportunities available to him. But he believes his CPP opened doors that would not have been available to him without the certification.

For example, he says the CPP allows him to jump into many conversations with others who are certified. Armed with the CPP, Dillon finds that other CPPs quickly take notice and conclude that he "knows what he is talking about."

Convergint Technologies has supported Dillon's participation in ASIS activities and encourages all colleagues to attain at least one ASIS certification. Dillon is convinced that achieving certification is worth the effort. "It will be the best learning experience, will allow for continued advancement, and will provide access to a new network of individuals," he says. "Just do it!"

Being involved in great experiences with genuine people has given Dillon a deep appreciation for his career. He advocates a similar path for others: "For those who like to see how businesses are run and products are manufactured, a career in the security industry provides access to the coolest companies and the opportunity to assist in solving their problems and address their daily concerns."

PROFILE BY **MARY ALICE DAVIDSON,** PRINCIPAL, DAVIDSON COMMUNICATIONS

seasoned veteran, the second edition of *The Manager's Handbook for Corporate Security* provides a comprehensive look at the past, present, and future of the security industry—a world that experiences both operational and functional changes at light speeds. Using a mythical organization called International Widget Corporation to illustrate problems and solutions, it creatively brings theory to life as it transforms the difficult concepts of "what should be" into "what is." Throughout the book, risk management is enlisted to transform security from a reactive process to a dynamic proactive endeavor.

The authors do a masterful job of taking the reader on a journey through various contingencies, and stress the importance of being proactive through key loss prevention programs, security awareness training, and developing strategic, tactical, and annual plans to combat risk and mitigate losses. Chapter after chapter, the authors emphasize that planning and preparedness strengthen the organization's overall security program and keenly integrate all layers within the organization. This approach helps solidify the security department's role in asset protection and keeps the security department where it should be—leading the effort. Adding value to an already solid effort, the authors consider new elements such as background checks, insurance, training, and cybersecurity—functions that are increasingly becoming part of the security department's portfolio.

The *Manager's Handbook for Corporate Security* is a must for any serious security professional and would be a valued addition to any security leader's professional bookshelf.

REVIEWER: *Terry Lee Wettig, CPP, is an independent security consultant who served 10 years as director of risk management with Brink's Incorporated. A retired U.S. Air Force chief master sergeant, he is currently a doctoral candidate specializing in organizational psychology. He is an ASIS member.*

#MYASIS: GET SOCIAL

ASIS wants to hear from you and learn what our members, chapters, and councils are doing. Share photos and news on Facebook, Instagram, or Twitter and tag with *#MyASIS*, and your story could be featured in future ASIS publications.

JUDICIAL DECISIONS

SURVEILLANCE. The U.S. government is shielded by sovereign immunity from a lawsuit claiming that an FBI agent used Bureau resources to spy on his wife, a U.S. court of appeals ruled.

Aida Gordo-González was married to an FBI agent when she discovered that he was using Bureau surveillance equipment to keep tabs on her, including GPS devices and video recording paraphernalia.

Gordo-González filed for divorce and, after it was finalized, she sued the U.S. government alleging that her ex-husband had "improperly used equipment belonging to the FBI and that his superiors were negligent in failing to supervise him adequately, thus allowing him to engage in inappropriate surveillance," according to court documents.

The government moved to have the case dismissed for lack of subject-matter jurisdiction, and a district court granted its request. Gordo-González appealed the dismissal to the U.S. Court of Appeals for the First Circuit, which took up the case.

The appellate court found that agency

ELSEWHERE IN THE COURTS

BOMBING

A jury convicted Ahmad Khan Rahimi on eight charges related to his execution and attempted execution of bombings in New York City and New Jersey on September 17, 2016, which injured more than 30 people and caused millions of dollars in property damage. The jury found Rahimi guilty of using a weapon of mass destruction, attempting to use a weapon of mass destruction, bombing a place of public use, destroying property by means of fire or explosive, interstate transportation and receipt of explosives, and two counts of using a destructive device to further a crime of violence. Rahimi's sentencing is scheduled for January 18, and he faces the possibility of multiple life in prison sentences. (*U.S. v. Rahimi*, U.S. District Court for the Southern District of New York, No. 16-CRIM-760, 2017)

EMAILS

The U.S. Supreme Court agreed to hear a case that could require Microsoft to turn over emails stored overseas to the U.S. government. Microsoft has been engaged in a legal battle with the U.S. government since 2013 when prosecutors demanded it turn over emails related to a drug-trafficking case. The emails in question were stored on servers in Ireland. Microsoft sued to block the request, claiming U.S. law enforcement could not seize evidence held in another country—even with a warrant. Microsoft lost its case, but appealed to the U.S. Court of Appeals for the Second Circuit, which declined to enforce the warrant. (*U.S. v. Microsoft*, U.S. Court of Appeals for the Second Circuit, No. 14-2985, 2017)

HACKING

The U.S. Supreme Court declined to take up cases on computer hacking, leaving in place a lower ruling that found that employees with legitimate access to employer systems cannot grant authorization to third parties to use them—only the computer system owner can do that. The decision upholds a jury ruling that convicted a recruiter for using another employee's password to access his former employer's database. (*Power Ventures v. Facebook*, U.S. Supreme Court, No. 16-1105, 2017; Nosal v. U.S., U.S. Supreme Court, No. 16-1344, 2017)

LEGAL HIGHLIGHTS

LEGISLATION

ISSUE: Fraud
BILL: P.L. 115-59
VENUE: U.S. Executive Branch
STATUS: Enacted
SIGNIFICANCE: Prevents U.S. federal agencies from including Social Security numbers on documents sent via mail unless the inclusion is necessary.

ISSUE: Human Trafficking
BILL: S. 1693
VENUE: U.S. Senate
STATUS: Under Consideration
SIGNIFICANCE: Would hold websites liable for information published on their sites that is "designed to facilitate sex trafficking."

officials should not allow unauthorized use of FBI equipment by agents.

But the law does not "direct the manner in which the supervision is to be carried out," court documents said. "Nor does it necessitate the taking of any specific action that the plaintiff plausibly might contend would have prevented her ex-husband's misuse of FBI equipment." (*Gordo-González v. U.S.*, U.S. Court of Appeals for the First Circuit, No. 16-2276, 2017)

DISCRIMINATION. Dash Dream Plant, Inc., will pay $110,000 and other relief to settle charges that it engaged in pregnancy discrimination when it allegedly told female workers to not get pregnant.

The U.S. Equal Employment Opportunity Commission (EEOC) claimed that through an investigation it found that Dash held staff meetings during which female employees were told to not get pregnant, and if they became pregnant they should consider themselves fired.

"The lawsuit also alleged that female employees were not reinstated or rehired when they attempted to return to work after childbirth," according to an EEOC press release.

The alleged conduct is a violation of Title VII of the Civil Rights Act of 1964, as amended by the Pregnancy Discrimination Act of 1978 and Title I of the Civil Rights Act of 1991.

The EEOC filed suit against Dash, which agreed to pay $110,000 to two former employees who said they were discriminated against to settle the charges. Dash will also retain an external equal employment opportunity monitor to assist it in creating, reviewing, and revising its policies and practices to ensure they are compliant with U.S. law.

The monitor will help Dash create a centralized tracking system for discrimination complaints, and prep semi-annual reports for the EEOC on Dash's progress and compliance. (*EEOC v. Dash Dream Plant, Inc.*, U.S. District Court for the Eastern District of California, No. 1:16-cv-01395-DAD-EPG)

REGULATIONS

United States

CRIME. U.S. Attorney General Jeff Sessions revived a U.S. President George W. Bush–era strategy to fight crime that emphasizes prosecutions of gun and gang crimes.

In a memo, Sessions said federal prosecutors would be evaluated based on their commitment to Project Safe Neighborhoods. The program focuses on trying individuals on gun crimes in federal court, which can issue longer sentences at prisons further away from the original area of jurisdiction.

"Taking what we have learned since the program began in 2001, we have updated it and enhanced it, emphasizing the role of our U.S. attorneys, the promise of new technologies, and above all, partnership with local communities," Sessions said in a press release. "With these changes, I believe that this program will be more effective than ever and help us fulfill our mission to make America safer."

As part of the program, Sessions is requiring each U.S. attorney to implement a plan based on five principles—leadership, partnership, targeted and prioritized enforcement, prevention, and accountability—to address the most significant violent crime in his or her district.

"This framework will enable each United States attorney, in collaboration with law enforcement and community partners, to develop a violence reduction plan that meets local needs, while leveraging the power of federal law and federal courts against the most violent offenders," Sessions said in a memo to U.S. attorneys.

CAMPUS SAFETY. The U.S. Department of Education Office of Civil Rights rescinded previous mandates issued during the Obama administration on campus sexual assault that required higher education institutions to take specific actions and meet reporting requirements on sexual assaults.

In a new mandate described in a Dear Colleague letter the department rescinded previous letters because they were "confusing and counterproductive" and "led to the deprivation of rights for many students—both accused students denied fair process and victims denied an adequate resolution of their complaints."

Revoking the letters means that schools no longer have to adopt a "minimal standard of proof" when investigating and disciplining students for sexual assaults. Schools now have the option to apply the "minimal standard of proof" or higher standards of proof:

ISSUE: Virtual Currency
BILL: H.R. 2433
VENUE: U.S. House of Representatives
STATUS: Passed
SIGNIFICANCE: Would direct the U.S. federal government to develop and disseminate a threat assessment about the threat posed by individuals using virtual currency to carry out terrorism.

ISSUE: Terrorism
BILL: H.R. 3284
VENUE: U.S. House of Representatives
STATUS: Passed
SIGNIFICANCE: Would direct the U.S. federal government to create a Joint Counterterrorism Awareness Workshop Series to address emerging terrorist threats.

the "clear-and-convincing-evidence standard," which means it's "more likely than not" that a sexual assault occurred; and the "highly probable or reasonably certain" standard.

The department will also develop a new approach to student sexual misconduct that "responds to the concerns of stakeholders and that aligns with the purpose of Title IX to achieve fair access to educational benefits," it said.

While the department said the new policy is designed to create a fairer process for sexual assault investigations, critics have claimed that it will discourage victims from reporting sex crimes.

DISCRIMINATION. Sessions rescinded a previous federal government policy that protected transgender workers from discrimination under Title VII of the 1964 Civil Rights Act.

"Title VII's prohibition on sex discrimination encompasses discrimination between men and women, but does not encompass discrimination based on gender identity per se, including transgender status," according to a memo from Sessions to the U.S. Department of Justice (DOJ) staff that was obtained by Buzzfeed.

"Although federal law, including Title VII, provides various protections to transgender individuals, Title VII does not prohibit discrimination based on gender identity per se," Sessions wrote. "This is a conclusion of law, not policy. As a law enforcement agency, the Department of Justice must interpret Title VII as written by Congress."

Critics, however, contend that Sessions' position ignores developments in case law, which has recently established that sex discrimination does include discrimination based on gender identity and sex stereotyping—meaning it's prohibited under Title VII.

EMAIL. The U.S. Department of Homeland Security issued a binding directive that requires all U.S. agencies to adopt email and Web security protections against phishing and spam.

All agencies were required to implement Domain-based Message Authentication, Reporting, and Conformance (DMARC) by January 2018. DMARC is a technical specification that is designed to stop unauthorized email uses of a domain in an effort to prevent email domain attacks, such as Business Email Compromise.

Agencies are also required to implement Hypertext Transfer Protocol Secure (HTTPS) for all .gov websites. HTTPS uses an encryption protocol that is designed to keep data safe when transmitted over the Internet, such as payment information in an e-commerce transaction.

FOR MORE INFORMATION:

U.S. CAPITOL SWITCHBOARD (INFORMATION):
202/224-3121

LEGISLATIVE STATUS OFFICE (STATUS OF BILLS):
202/225-1772

To see the full text of selected regulations, bills, and reports, visit ***www.securitymanagement.com*** *and click on SM Online.*

LEGISLATION

California

GENDER. California Governor Jerry Brown signed legislation into law that allows state residents to choose between one of three gender options on official documents.

The Gender Recognition Act (formerly S.B. 179) allows California residents to select male, female, or nonbinary—an intersex option—on official documents, including driver's licenses. California's registrar will then issue new birth certificates to residents born in the state who wish to identify as nonbinary.

The law also eliminates a previous requirement that residents undergo treatment and submit a sworn statement from a physician to change their gender identity.

With the law's enactment, California joins Oregon and Washington, D.C., in allowing residents to identify as an intersex option on driver's licenses.

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

LEGAL HIGHLIGHTS

COURT CASES

ISSUE: OPM Breach
CASE: *In Re: U.S. Office of Personnel Management*
VENUE: U.S. District Court for the District of Columbia
STATUS: Dismissed
SIGNIFICANCE: The judge found that because the OPM data was stolen, not disclosed, plaintiffs had not suffered harm and did not have standing to sue the agency.

ISSUE: Discrimination
CASE: *EEOC v. Vicksburg Healthcare, LLC*
VENUE: U.S. District Court for the Southern District of Mississippi
STATUS: Settled
SIGNIFICANCE: Vicksburg Healthcare will pay $100,000 to settle a disability discrimination suit alleging it failed to provide accommodation for an employee to return to work after surgery.

LET YOUR VOICE BE HEARD. WITHOUT SAYING A WORD.

FOLLOW US ON SOCIAL MEDIA

SECURITY
MANAGEMENT

Follow us on facebook at:
facebook.com/SecMgmtMag

Follow us on twitter at:
@SecMgmtMag

Keep in touch with *Security Management* – digitally. Voice your opinions by commenting or tweeting. You can also like us or follow us to get up-to-date notifications about breaking news, events, and access to the invaluable content *Security Management* provides online and in print.

AIRPORT CONNECTIONS

OSLO AIRPORT, GARDERMOEN, is Norway's largest and Scandinavia's second largest airport, handling 26 million passengers in 2016. The airport had an analog communication system in the air traffic control tower, and wished to upgrade to an IP system that would provide operational analytics and error reporting of critical communications, redundancy for high availability and reliability, and integrated operational, passenger, and emergency communications capabilities. The communication devices also needed to stand up to dynamic ranges of noise and—outside the terminal—a variety of weather conditions.

Zenitel had worked with the airport in the past, and stepped up to provide the updated system, including TMIS-1 Turbine Mini Intercoms that plug and play with the airport's IP telephone system, as well as TCIS-4 Turbine Intercom Stations to support intelligibility, interoperability, and reliability standards of the airport. Passengers and airport personnel can easily use the devices for communications. In emergencies, the system provides direct and clear notifications to all parts of the airport.

PARTNERSHIPS AND DEALS

Software House, part of Johnson Controls, and **Allegion** are extending their partnership to include the pairing of Schlage LE and NDE wireless locks with Software House C•CURE 9000.

Arteco Video Event Management and Video Intelligence Solutions are now compatible with the new **Hanwha Techwin** Wisenet 5 chipset.

Top Notch Distributors is stocking an extensive inventory of **ASSA ABLOY** products, parts, and accessories in four U.S. locations.

IndigoVision incorporated **BriefCam** technology as part of its Control Center v15.0 security management solution.

Dataguise welcomed **Computacenter** to the Dataguise partner community.

Nuvias is the sole pan-EMEA distributor for **Dtex Systems** insider threat solutions.

ISONAS Inc. integrated its newest software application, Pure Access, with XProtect Access from **Milestone Systems.**

The **University of Iowa Hospitals and Clinics** unified its security operations with the deployment of victor and C•CURE 9000 security management platform from **Johnson Controls.**

Just Add Power announced partnerships with **Tandem Marketing** and **Synapse Sales & Marketing** to broaden its product support across the United States.

March Networks and **Patriot One Technologies Inc.** announced an integration that offers video-enabled covert weapon detection notifications.

For two decades, **Mercury Security** and **Open Options** have collaborated to deliver security systems to customers all over the world.

MONI Smart Security will provide a professional monitoring service for **Nest Secure.**

Nozomi Networks announced a new partnership with **FireEye** to pro-

vide next generation ICS security that extends visibility across IT and OT environments.

D-Tools, Inc., joined the **PSA** Business Solutions Providers, offering its estimation, system design, and project management software platform to PSA members and owners.

Zurich-based **Sunrise Communications AG** will implement cloud-based security technology from the German firm **Secucloud.**

SecuraTrac now integrates with **Micro Key Systems** and is introducing a version of its Mobile Defender Model S that works on the Verizon network in addition to AT&T and T-Mobile networks in more than 120 countries.

Setracon Incorporated announced the award of a pilot project providing enterprise security risk management services for **General Atomics.**

University of Georgia worked with **Spectra Logic** to implement a disaster recovery archive strategy, installing Spectra tape libraries, a converged storage system, and a disk solution to protect content.

V5 Systems was selected by **Pelco by Schneider Electric** for integration with its V5 Camera Adaptive Platform.

VIVOTEK formulated an IP surveillance solution for **Varun Beverages.**

Our Lady of Perpetual Help in Ellicott City, Maryland, installed a **VIZpin** smartphone access control system that allows parishioners to enter the building for prayer most times of day.

Imperial Oil is expanding its use of 3D Perspective scanners from **VOTI DETECTION** to provide enhanced security and threat detection.

GOVERNMENT CONTRACTS

French water utility **Eau de Valence** chose **ASSA ABLOY**'s key-based access control technology, CLIQ, to replace its mechanical locking system.

Canon U.S.A., Inc., sold its 300th unit of the RadPRO SecurPASS Full Body Security Screening System to **Clay County Jail** in Manchester, Kentucky.

Maldives Immigration worked with **DERMALOG** to create an ID card that can be used for payments, as a driver's license, as a health and insurance card, and as a passport.

Daytona Beach Police Department used drones from **DJI** to conduct pre- and post-storm assessments of Hurricane Irma.

FLIR Systems, Inc., received an order to deliver Tac Flir surveillance cameras in support of the **U.S. Army** EO/IR-Force Protection program.

Frequentis and **Hexagon Safety & Infrastructure** were selected to supply mission-critical technologies for the **ELKOS Austria** project, a nationwide, unified command and communication system.

IDenta Corp. was approved as an official supplier for the **European Union.**

ISV Redwall Technologies is working with the **U.S. Department of Defense** on a project centered around mobile data integrity and confidentiality.

Janus Global Operations will provide risk management and security for the **European Union** organization working to help build maritime civilian law enforcement in Somalia.

Port Hedland in Australia chose the SharpEye SBS-900 X-Band radar system from **Kelvin Hughes,** which will be installed as part of a complete VTS system by **AMS Group.**

L3 Technologies announced that its ProVision 2 advanced passenger screening system has been purchased by the **Istanbul Ataturk Airport.**

Orolia, through its McMurdo brand, announced that the **U.S. Coast Guard** has activated a contract for up to 16,000 FastFind 220 Personal Locator Beacon units.

SparkCognition is providing collaborative thought leadership on the role of artificial intelligence in future warfare to the **British Army.**

UltiSat, Inc., announced that **U.S. Defense Information Systems Agency** Defense Information Technology Contracting Organization awarded a task order for UltiSat to provide satellite services support for Global Hawk Unmanned Air Vehicle operations.

Alaska's **Anchorage School District** implemented a districtwide networked security monitoring system to address rising vandalism such as broken windows and recurring playground fires at elementary schools. The system is based on technology from **Milestone Systems**.

The **Republic of Zambia** awarded **Veridos** a contract to deliver polycarbonate electronic ID cards to Zambia. The **Police Grand-Ducale Luxembourg** commissioned Veridos to install ten eGates for automated border control at the country's international airport.

The **U.S. Air Force** expanded its partnership with **VOTI DETECTION** as the preferred security screening system on bases worldwide.

AWARDS AND CERTIFICATIONS

Agent Video Intelligence holds the largest market share of video analytics software, according to **IHS Markit.**

Allied Universal received two Outstanding Security Performance Awards: Outstanding Customer Service Initiative for the UCHealth Patient Watch Program and Outstanding Contract Security Officer for Site Supervisor Zach Ostergren.

Asurion was honored by **Frost & Sullivan** with the 2017 North American Product Leadership Award for Mobile Protection Services.

National Cyber Security Centre—Finland granted approval for the **Bittium** Tough Mobile LTE-smartphone and related Bittium Secure Suite back-end system to process material that is classified nationally as Confidential.

Concurrent Technologies Corporation's Johnstown, Pennsylvania facilities have been recertified under the **Occupational Safety and Health Administration** Voluntary Protection Programs as a Star site.

ControlScan was approved by the **Payment Card Industry** Security Standards Council (PCI SSC) to extend its Qualified Security Assessor (QSA) services to companies operating in Canada.

D-Link announced that its Smart Managed PoE Powered 5-Port Gigabit Switch received the 2017 New Product of the Year Award from ***Security Today*** in the Networking Support Solutions category.

Honeywell's BW Clip4 portable gas detector won the 2017 New Product of the Year in the Industrial Hygiene category from ***Occupational Health & Safety*** magazine.

Janrain obtained **Cloud Security Alliance** Level 2 (CSA) STAR Certification and **ISO** 27018:2014 certification for handling personally identifiable information.

Along with partner **Video Analysis Solutions, Oncam** won Most Innovative In-store Solution as part of **Retail Risk** Fraud Awards 2017.

OutSystems received ISO 27001, ISO 22301, and SOC 2 certifications.

Attendees at the 2017 **ASIS International** Annual Seminar and Exhibits voted the **Pelco by Schneider Electric** VideoXpert Professional Video Management System the ASIS Accolades People's Choice Award winner. The Judges Choice awardee was the Cobalt intelligent security robot from **Cobalt Robotics.** Find the rest of the winners via SM Online.

RiskIQ won the Overall Web Security Solution Provider of the Year award from **CyberSecurity Breakthrough.**

Vaultive received a new patent relating to its ability to allow organizations to use cloud-hosted email while reducing the exposure of sensitive data.

Virtual StrongBox, Inc., earned two patents that recognize the way it gathers information from the digital consumer and protects that data.

STRATEGIC MOVES IN THE NEWS

WHO	WHAT	OF/WITH	RESULT
ASSA ABLOY	*ACQUISITION*	**MERCURY SECURITY**	The acquisition improves the company's position in physical access control and will provide growth opportunities, especially for the HID Global brand.
EVERBRIDGE	*PARTNERSHIP*	**G4S**	G4S will use Everbridge products in combination with its own security services and software to deliver new integrated security services and solutions.
ADDSECURE	*ACQUISITION*	**CHIRON**	This is a step towards AddSecure's goal to be the leading supplier of secure communication for alarm and IoT solutions in Europe.
THREATQUOTIENT	*PARTNERSHIP*	**PHANTOM**	The companies will automate the full incident response workflow, including preparation, detection and analysis, containment, eradication, and recovery.

ANNOUNCEMENTS

Acuant acquired the Ozone line of identity products, intellectual property, and talent from **Mount Airey Group.**

Akamai Technologies, Inc., entered into an agreement to acquire **Nominum,** which provides enterprise security solutions for carriers.

AMG Systems participated in a trade delegation to the Baltic states organized through the **United Kingdom Department for International Trade.**

Anixter University offers an array of technical and standards-based information for contractors, integrators, end users and consultants.

ASSA ABLOY partnered with the **USO** to provide backpacks loaded with food and personal items for veterans returning from deployment. The 1,000 backpacks were packed on the show floor of ASIS 2017.

Carleton University, along with **Queen's University** and **Cyberspark,** launched Global EPIC, a new international cybersecurity initiative designed to combat growing world challenges by facilitating global collaboration.

CNL Software is moving its U.K. headquarters to larger premises in Watchmoor Park, Camberley, Surrey.

Dahua Technology established Dahua Technology Rus as a subsidiary in Moscow.

Dragos is a National Cybersecurity Excellence Partner with the **National Cybersecurity Center of Excellence.**

FirstNet and **AT&T** launched a developer program to help equip first responders with state-of-the-art communications tools.

Forensic Logic acquired the COPLINK suite of products from **IBM.**

Gallaher released a new website, gallahersafe.com, in honor of its 44th year in business.

Gillmore Security Systems, Inc., acquired four Ohio companies: **Digital Security, Courtland Security, Gen-X, Santee Security,** and **Buckeye Electronics & Security Technology.**

The **Institute for Critical Infrastructure Technology** introduced the Center for Cyber-Influence Operations Studies to examine the weaponized digital applications used by foreign nation-states for influence operations.

Iron Mountain Incorporated opened a new information management facility in Mabelvale, Arkansas.

JLT Cyber Risk Consortium developed a research and thought leadership hub exploring cybersecurity threats.

Johnson Controls sold its Scott Safety business to **3M.**

Mimecast Limited will expand into Germany with a new office in Munich.

Pinkerton launched its 2017 Risk Index Report, *A World Ranking of Business Risk.*

PRAESIDIAD relocated its corporate headquarters from Ghent, Belgium, to London as part of a global access and communication strategy.

Pryme opened an Indiana Distribution Center and two satellite sales offices in Nevada and Arizona.

Safer Places, Inc., opened a new office in Portland, Maine.

Physical security specialist **Safetell** revamped its website to help users easily identify their security needs.

SmartRiskSolutions GmbH published a handbook on crisis management and crisis communications during a terrorist or active shooter attack. Find it via SM Online.

Stratfor announced a set of joint initiatives with the **Clements Center for National Security; the Robert Strauss Center for International Security and Law;** and the Intelligence Studies Project at **The University of Texas at Austin** to engage on geopolitical analysis, national security conversations, and graduate education.

VOTI DETECTION unveiled a company-wide rebrand including a name change from **VOTI Group** to **VOTI DETECTION,** website redesign, and more.

SECURITY SOFTWARE

SUREVIEW SYSTEMS of Tampa, Florida, added a new mapping solution for its Immix Command Center Physical Security Information Management (PSIM) platform. The new Immix geospatial-mapping interface allows users to better comprehend physical location information. The use of static facility floor plans overlaid directly onto the powerful Google Maps interface dramatically increases ease of use and accuracy. SureView has further leveraged this geospatial awareness to automatically associate the nearest cameras to an alarm, eliminating the need to preprogram links between devices. The ability to make these links on the fly delivers accurate and immediate situational awareness for remote operators, allowing them to efficiently respond during potentially chaotic situations. **101**

WALL RACK

The new ERWEN-12E750 19-inch wall rack enclosure from **VIDEO MOUNT PRODUCTS** of Stevensville, Maryland, has the added depth needed for installing today's deeper components. It has adjustable four-post rails, a removable hinged wall plate, reversible tempered glass front door, and optional fans for enhanced thermal management. It also offers welded steel construction, a vented top and bottom, top and bottom cable routing knockouts, reversible hinged front door, removable hinged back panel, and removable locking side panels. The 24-inch-deep unit holds up to 120 pounds of equipment. **102**

WATERPROOF DOOR SWITCHES

DORTRONICS SYSTEMS, INC., of Sag Harbor, New York, introduced a new line of waterproof pushbutton switches in the WR5276-HDD Series. They feature an IP66 rating and a neoprene gasket for use in harsh operating conditions such as outdoors and cleanrooms that require washdowns. They can be configured for card access systems or automatic door openers. The switches' double-pole, normally open, dry contact outputs can be wired to signal a door to unlock and the door opener to activate. The switches are made from brushed stainless steel in standard switch plate sizes with engraved legends. Custom plates are also available. **103**

Best Sellers Published by ASIS

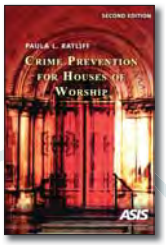
ACTIVE SHOOTER:
A HANDBOOK ON PREVENTION, 2ND ED.

Joshua Sinai, Ph.D.

In this expanded second edition, extensive new material includes an expanded matrix on the seven phases of an active shooter event, components involved, updated chronologies of active shooter incidents, timeframes perpetrators use to 'go operational', and more.
Intended for all those involved in public safety, whether in government, law enforcement, or the private sector.

184 pp., 2016, Spiral bound **Item No. 2271** **$65** **$45 members**
Also available on Kindle from Amazon.com.

CRIME PREVENTION FOR HOUSES OF WORSHIP, 2ND ED.



Paula L. Ratliff

Reading this book will assist you in developing awareness, identifying areas of prevention, and formulating a response to crime when it does occur so that your congregation may enjoy a safe environment in which to worship.

262 pp., 2015, SCVR **Item No. 2248** **$65** **$45 members**
Also available on Kindle from Amazon.com.

IMPLEMENTING PHYSICAL PROTECTION SYSTEMS:
A PRACTICAL GUIDE, 2ND ED.

David G. Patterson, CPP, PSP

The purpose of this book is to guide security professionals in implementing physical protection systems (PPSs). It is also intended as study material for the ASIS Physical Security Professional (PSP) certification examination.

208 pp., 2013, SCVR **Item No. 2063** **$50** **$35 members**
Also available in Spanish and on Kindle from Amazon.com.

PHYSICAL SECURITY PRINCIPLES

PSP

Michael E. Knoke, CPP, Managing Editor;
Kevin E. Peterson, CPP, Co-Editor

This book was written with three key purposes: for security professionals worldwide to have a valuable desk reference on aspects of the practice of physical security; it may be an appropriate text for college courses related to physical security as comprehensive reference for those interested in pursuing a certification in physical security.

582 pp., 2013, HCVR **Item No. 2251** **$269** **$189 members**
582 pp., 2013, SCVR **Item No. 2251S** **$189** **$129 members**
Also available in Spanish and on Kindle from Amazon.com.

PROFESSIONAL INVESTIGATOR'S MANUAL

PCI

Michael E. Knoke, CPP, and
Edward P. De Lise, CPP, Editors

This guide explores the knowledge necessary to be a successful investigator and prepares you for the Professional Certified Investigator (PCI) examination. Topics covered include: investigations management, interview and interrogation, undercover investigations, due diligence, and basics of preemployment background screening. The chapters on evidence and testimony offer insights often taken for granted.

344 pp., 2010, HCVR **Item No. 1880** **$175** **$105 members**
346 pp., 2010, SCVR **Item No. 2069** **$93** **$64 members**
Also available in Spanish and on Kindle from Amazon.com.

PROTECTION OF ASSETS (POA)

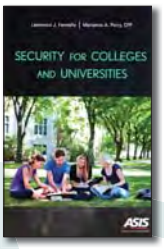
CPP

ASIS International

POA is considered the premier reference for the security industry. Written, edited, and peer-reviewed by security subject matter experts, this comprehensive source covers all aspects of security. *POA* is available as an online subscription, an eight-volume set, and as individual books.
For pricing and to order, visit *www.protectionofassets.com.*

Also available in Spanish and on Kindle from Amazon.com.

SECURITY FOR COLLEGES AND UNIVERSITIES



Lawrence J. Fennelly and Marianna Perry, CPP

Security threats at colleges and universities have changed tremendously in the last decade. Mass shootings, bomb threats, assaults, thefts, and other dangers challenge institutions in their responsibility to provide a safe environment. This book presents timely solutions to difficult problems. Topics include best practices, risk management, sexual assault, target hardening, technology, and many more.

246 pp., 2014, SCVR **Item No. 2208** **$60** **$42 members**
Also available on Kindle from Amazon.com.

SECURITY IN 2025

Lawrence J. Fennelly, Mark Beaudry, PhD, CPP,
and Marianna Perry, CPP, Editors
ASIS International

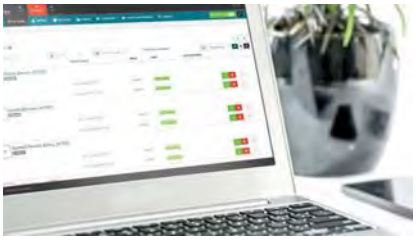
Security in 2025 employs a modern technique to peer into the future—crowdsourcing a vision from the minds of 34 security professionals, from entry-level to veterans in the field. It offers predictions on a wide range of current and emerging issues that will impact security in the next decade—cyber fraud, security officer training, kidnapping/human trafficking, terrorism trends, drones, the future of corporate loss prevention, and so much more. An invaluable resource for security professionals and students alike.

260 pp., 2017, SCVR **Item No. 2317** **$68** **$48 members**
Also available on Kindle from Amazon.com.

To purchase or browse titles, visit
asisonline.org/asisbest

IDENTITY MANAGEMENT

AMAG TECHNOLOGY of Torrance, California, introduced Symmetry CONNECT, a policy-based identity management platform that ensures that only individuals with approvals and requirements have access to secure areas for the timeframe needed, providing security as well as compliance. The platform automates workflows to streamline key processes involved in managing the diverse identities across an organization. Designed for new and existing Symmetry Access Control software users, CONNECT operates on most PCs, tablets, and smartphones. It is available in several formats for North American customers: as a cloud-hosted solution, hosted by AMAG in a secure monitoring center, or as an on-premise identity management solution installed at the end user's premise or data center. **104**



SAFETY APP

OMNIGO SOFTWARE of St. Louis, Missouri, arms protectors with a full suite of tools for seeing a bigger picture of security, putting powerful data at their fingertips and equipping them to make quicker, more informed decisions. The company recently launched Blert!, which empowers college students to instantly and anonymously report incidents from their mobile phones—via text, photo, or video—as easily as sending a text message or sharing a Snapchat video. The Blert! dashboard allows campus safety directors to monitor reports and instantly communicate with students who initiate a report. **107**

FIRE ALARM SYSTEM

The Taktis fire detection and alarm system from **KENTEC ELECTRONICS LTD.** of Dartford, United Kingdom, combines the latest hardware and software to produce a powerful control and indication system. Certified to EN54-2 and EN54-4, the system is ideal for installation in larger buildings because up to 128 panels and repeaters can be networked. Its integrated touchscreen interface and QWERTY keyboard make it simple to use and understand. Multiple protocol support on one panel (in banks of two loops) gives full flexibility and it displays clear information so that when an event occurs, appropriate action can be taken. It supports a 10,000-entry log with filtering that records system activity down to event type, dates, zone, panel, and address. **105**

ATTACK DETECTION

New from **ARUBA**, a Hewlett Packard Enterprise Company, is the Aruba 360 Secure Fabric, a security framework that provides analytics-driven attack detection and response. IntroSpect uses machine learning analytics to reduce the time and effort required to identify and resolve cyberattacks. IntroSpect automatically creates a Risk Profile for every user, system, and IoT device connected to the network. When a Risk Score reaches a predefined level, a policy from Aruba ClearPass can be triggered to take enforcement actions to stop the attack and provide additional time to investigate. Identifying and resolving security incidents is reduced to minutes, compared to hours and days via manual methods. **106**

FACIAL RECOGNITION

DIGITAL BARRIERS PLC of Ashburn, Virginia, introduced SmartVis Identifier, a live facial recognition system for body-worn law enforcement cameras. The integration of the company's EdgeVis mobile live streaming solution and SmartVis technologies provides defense, security, and law enforcement agencies with real-time facial recognition against multiple watch lists and databases. The system is designed to meet operational requirements of users. Removing human error from the equation and plugging resourcing gaps, it enables organizations to widen deployments of facial recognition to enhance security and public safety, with persons of interest highlighted in real time. **108**

ASIS INTERNATIONAL
Advancing Security Worldwide®

ADVANCE

YOUR PROFESSIONAL DEVELOPMENT IN 2018. JOIN ASIS IN ORLANDO, FLORIDA.

Professional development is a key driver for career advancement. In addition to staying on top of the latest threats and risk management strategies, a solid understanding of core security principles and field-tested best practices is essential. This is the type of vital information you'll find in our March line-up of educational programming in Orlando.

CPP Review Program

March 12-13, 2018

This program provides 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

March 12-13, 2018

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)

March 12-15, 2018

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!

Learn more and register at asisonline.org/education

SAVE $100
WHEN YOU REGISTER BY JANUARY 27, 2018.

REGISTER TODAY!

VIDEO MANAGEMENT

TYCO SECURITY PRODUCTS of Westford, Massachusetts, released exacqVision 8.8, which provides powerful tools that improve situational awareness and control. Some features include simplified camera configuration, Web and mobile improvement, support for higher-resolution displays, additional third-party camera options, and H.265 support for Illustra IP cameras. With enhanced event linking, operators can display any event linkage as association to appear on top of the live video feed. This is useful, for example, in retail applications to detect foil-lined bags popular with shoplifters. Controls for administrators help them manage how and when users can access the system, monitor inactive accounts, create temporary guest accounts, and expand access to preset tours. **109**

CLOUD SECURITY MANAGEMENT

S2 SECURITY of Framingham, Massachusetts, introduced S2 Cumulus, a new cloud-based service that connects the S2 ecosystem, enabling administration and monitoring of S2 products as well as critical communication between people, devices, and third-party systems. It is a backbone for providing new cloud services to integrators and end users. It offers system health monitoring, software license management, remote software updates, and automatic alerts to changes in system status. Leveraging the cloud, S2 Cumulus will enable S2 Security to develop and provide services such as virtual credential acquisition and management, video stream sharing, remote mustering, communication with third-party systems, and more. **110**

TRANSFER SWITCH

POWER DISTRIBUTION, INC., of Richmond, Virginia, announced its new WaveStar TFA Static Transfer Switch. A true front-access STS cabinet, it offers an improved footprint, faster installation, and increased worker safety during data center power maintenance procedures. Static transfer switches facilitate uninterrupted power to a data center's electrical load, overcoming the unreliability of conventional electrical distribution systems by switching to a redundant power path in the event of a failure. Legacy designs present a maintenance safety challenge because live electrical components are not separated from other areas. Too often electrical arcs cause device damage, unplanned downtime, or endanger a worker's safety. This cabinet separates live electrical components into individual compartments, optimizing routine maintenance and simplifying installation and infrared scanning. **111**

PSIM SITUATION MANAGEMENT

CNL SOFTWARE of Ashburn, Virginia, released version 5.5 of its IPSecurityCenter physical security information management (PSIM) system software. The release includes many performance and feature enhancements for large-scale and mission-critical deployments. The latest version addresses PSIM system deployment challenges through features that include federated hub and node architecture, central management, enhanced plug-in framework, maintenance management, automated software upgrades, and more. Auditing and management data functions create records of all operator activity to assist with regulatory compliance. **112**

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

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

ADVERTISERS ONLINE

Abloy Security, Inc.
www.abloyusa.com

Axis Communications
www.axis.com

Commport Technologies
www.comm-port.com

Detex Corporation
www.detex.com/imablur6

Digitize, Inc.
www.digitize-inc.com

dormakaba
go.dormakaba.com/PAS-SMMag

DSI (Designed Security Inc.)
www.dsigo.com

DSX Access Systems, Inc.
www.dsxinc.com

G4S
www.g4s.us

GAI-Tronics Corporation
www.gai-tronics.com

Garrett Metal Detectors
www.garrett.com

Hikvision USA
www.hikvision.com

Mission 500
www.mission500.org

Research Electronics, Int'l
www.reiusa.net

SecurAmerica
www.securamericallc.com

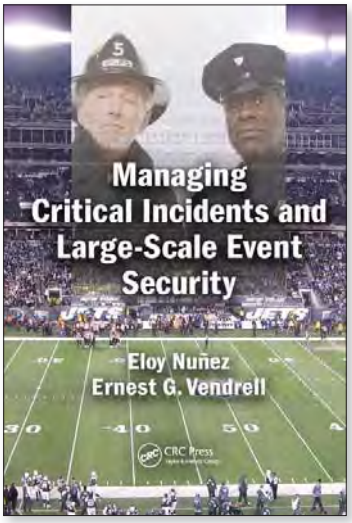
Special Response Corporation
www.specialresponse.com

SRG Security Resource Group Inc.
www.securityresourcegroup.com

TSCM America
www.tscmamerica.com

EVENT SECURITY

THE ASIS 2017 BOOK OF THE YEAR IS *MANAGING CRITICAL INCIDENTS AND LARGE-SCALE EVENT SECURITY* BY **ELOY NUÑEZ** AND **ERNEST G. VENDRELL.** THE AUTHORS SPOKE TO *SECURITY MANAGEMENT* ABOUT SECURITY TRENDS AND CHALLENGES IN THE EVENT INDUSTRY.



Q. WHAT ARE SOME OF THE BIGGEST CHALLENGES FACING THE EVENT SECURITY INDUSTRY TODAY?

A. An overreliance on technology is a major challenge. We tend to think that a wall or a fence will keep the bad guys out, and it does help a lot, but in and of itself it's not going to solve our problems. We know that every fence and wall can be breached, and every technology that one can think of can be counteracted. It takes an active observation of the technology and how it's working. Another challenge is a sense of complacency–the idea that someone else is watching. That tends to make us less alert. Communication also becomes so important, especially when you're dealing with a variety of participants. It's essentially impossible to achieve requisite levels of coordination and collaboration without that effective communication.

Q. HOW HAS THE EVENT SECURITY SPACE EVOLVED OVER THE LAST FEW DECADES?

A. Three factors have made us more effective and efficient than in the past: computer processing speed, the miniaturization of technology, and the interconnectedness of people via devices. The improvements to technology have been outstanding. We're now able to process information more quickly. The interconnectedness allows us to communicate, collaborate, and crowdsource for information. There are so many different people from disparate backgrounds and agencies. We all get together and plan things out, and the byproduct is that we learn from each other.

Q. YOUR BOOK DRAWS ON LESSONS LEARNED FROM PAST EVENTS. WHAT ARE SOME OF THE OVERARCHING THEMES IN THOSE LESSONS?

A. Given the complexities of critical incident management and large-scale event planning, we try to simplify things as best we can so that everyone is able to execute those plans. It takes a well-trained, diversified, and committed team that has clear goals and objectives. Have the team that you put in place practice as much as possible, and institute training that's relevant, realistic, and replicates the environment that you're working in.

Q. GIVEN THE RANGE OF THREATS TO THE LIVE EVENT INDUSTRY, HOW CAN SECURITY PROFESSIONALS SHARE INFORMATION TO HELP MITIGATE THOSE CHALLENGES?

A. Networking is so critical. One thing we wrote about was that, in the public safety arena, we were great at identifying lessons learned, but the problem was that we weren't applying those lessons. Conferences like GSX (formerly the ASIS annual seminar and exhibits), where you have professionals sharing lessons learned and how they applied them, are so important in terms of professionalization and collectively doing a better job moving forward. Identifying contacts ahead of time and getting to know them before there's a problem is critical. That way when an unforeseen incident occurs, you have the right parties on speed-dial.

Visit SM Online for the full interview.

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

MISSION 500

CREATING THE FUTURE OF SECURITY . . . TODAY

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 the 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 systems in the world, choose the total security relationship with DSX.

- No "Per Seat" Licensing In System Pricing
- LAN/WAN Compatible
- Smart Card and Biometric Integration
- Unlimited Access Levels Per Cardholder
- Integrated Photo ID Badging
- Backup SQL Server

DSX Access Systems, Inc.

www.dsxinc.com

10731 Rockwall Road | Dallas, TX USA 75238-1219
888.419.8353 | 214.553.6140 | sales@dsxinc.com

- Backwards Compatible Architecture
- Alarm Text Message/ E-Mail Notification
- Hot Swap Redundant Communication Server
- High Level Elevator Control Interface
- Integrated Wireless Locksets

Quality. Reliability. Integrity. The Security Professionals' First Choice.