Issue & Beyond

- **Fraud**
  Swindles of all types are on the rise.

- **Infrastructure**
  Puerto Rico begins repairing its power grid.

**28**
DATA COMPLIANCE

**44**
LIABILITY

**50**
COACHING

**32**
INVESTIGATING HARASSMENT
FRANK ARGENBRIGHT, SECURITY GUARD WANNABE
MY APOLOGIES

I owe an apology to the CEOs of the Big Four Guard Companies. My Security Guard Tap Out Charity Challenge was well-intended, but maybe not fair! Originally, my Security Guard Challenge to raise $1,000,000 for charity seemed like a great idea. I thought the four CEOs would have loved to participate.

Why? One, we would be able to recognize our security officers, the “boots on the ground”, as the most important people in our companies. Two, it would raise $1,000,000 for charity. Three, the five of us could have some fun going back to our roots. And four, on a personal basis, I would get one on one time with the four smartest and most successful guys in the security industry; it would have been a life’s dream!

However, after hearing confidentially from a number of you who work for the Big Four, it wasn’t a fair challenge. Bottom line, I was told you guys don’t have the time to commit to “such a menial task as a security guard post”. I was told the Four CEOs report to either private equity or a public company and have very tough jobs. As one of you said, he spends his day being told by private equity to cut, cut, cut, and increase margins, margins, margins, and we have to sell in 3 years, no later than 5 years. What a tough job.

So I personally apologize to the CEOs of the Big Four for my unfair challenge to you.

So please accept a $5,000 donation being made in each of your names to the ASIS Foundation. The money was donated in February.

P.S. - I am glad I don’t have your bosses! I just have to get my wife’s permission, though she can be tough; we’ve been married 39 years.
One day.

314 incidents.

314 right decisions.

When you’re responsible for the safety and security of a public transportation system involving hundreds of stations, the amount of incidents to detect, evaluate and act on every day is staggering. Wouldn’t you want a central surveillance system with smart tools to help you quickly and confidently make the right decisions? Minimize vandalism and service disruptions with tools like automatic alerts and sharable live video from all parts of the transit system— all with HDTV clarity.

Sounds good, right? We’ve made sure our network video solutions can handle it all. So you can make the right decision— for every incident.

Get the details at www.axis.com/stations
Signs that read “no weapons” in parking lots are illegal in some U.S. states in certain circumstances.

Eddie Sorrells, CPP, PCI, PSP, on legally handling weapons in the workplace.

PAGE 48

“IT’S LIKE A TRUCK FAST APPROACHING US.”

Ann LaFrance, partner and coleader of Squire Patton Boggs’ Data Privacy and Cybersecurity practice, on the upcoming European Union General Data Protection Regulation (GDPR) compliance deadline.

PAGE 28

Security Management

The number of fires in which the New York City Fire Department has used drones for imaging since purchasing them in March 2017.

PAGE 25

Anthony McGinty, CPP, of CSRA, Inc., discussing the challenges of in-flight disputes aboard aircraft.

PAGE 70

200,000

The number of people who had left Puerto Rico due to damage caused by Hurricane Maria, as of January 2018.

PAGE 21

“Short of placing a security officer on board, solutions may involve institutional changes in the flight crew-to-passenger relationship.”

Anthony McGinty, CPP, of CSRA, Inc., discussing the challenges of in-flight disputes aboard aircraft.

PAGE 70

“The number of fires in which the New York City Fire Department has used drones for imaging since purchasing them in March 2017.”

PAGE 25

26

The number of fires in which the New York City Fire Department has used drones for imaging since purchasing them in March 2017.

PAGE 25

200,000

The number of people who had left Puerto Rico due to damage caused by Hurricane Maria, as of January 2018.

PAGE 21

“IT’S LIKE A TRUCK FAST APPROACHING US.”

Ann LaFrance, partner and coleader of Squire Patton Boggs’ Data Privacy and Cybersecurity practice, on the upcoming European Union General Data Protection Regulation (GDPR) compliance deadline.

PAGE 28

200,000

The number of people who had left Puerto Rico due to damage caused by Hurricane Maria, as of January 2018.

PAGE 21

“IT’S LIKE A TRUCK FAST APPROACHING US.”

Ann LaFrance, partner and coleader of Squire Patton Boggs’ Data Privacy and Cybersecurity practice, on the upcoming European Union General Data Protection Regulation (GDPR) compliance deadline.

PAGE 28

200,000

The number of people who had left Puerto Rico due to damage caused by Hurricane Maria, as of January 2018.

PAGE 21

“IT’S LIKE A TRUCK FAST APPROACHING US.”

Ann LaFrance, partner and coleader of Squire Patton Boggs’ Data Privacy and Cybersecurity practice, on the upcoming European Union General Data Protection Regulation (GDPR) compliance deadline.

PAGE 28

200,000

The number of people who had left Puerto Rico due to damage caused by Hurricane Maria, as of January 2018.

PAGE 21

“IT’S LIKE A TRUCK FAST APPROACHING US.”

Ann LaFrance, partner and coleader of Squire Patton Boggs’ Data Privacy and Cybersecurity practice, on the upcoming European Union General Data Protection Regulation (GDPR) compliance deadline.

PAGE 28

200,000

The number of people who had left Puerto Rico due to damage caused by Hurricane Maria, as of January 2018.

PAGE 21

“IT’S LIKE A TRUCK FAST APPROACHING US.”

Ann LaFrance, partner and coleader of Squire Patton Boggs’ Data Privacy and Cybersecurity practice, on the upcoming European Union General Data Protection Regulation (GDPR) compliance deadline.

PAGE 28

200,000

The number of people who had left Puerto Rico due to damage caused by Hurricane Maria, as of January 2018.

PAGE 21

“IT’S LIKE A TRUCK FAST APPROACHING US.”

Ann LaFrance, partner and coleader of Squire Patton Boggs’ Data Privacy and Cybersecurity practice, on the upcoming European Union General Data Protection Regulation (GDPR) compliance deadline.

PAGE 28

200,000

The number of people who had left Puerto Rico due to damage caused by Hurricane Maria, as of January 2018.

PAGE 21

“IT’S LIKE A TRUCK FAST APPROACHING US.”

Ann LaFrance, partner and coleader of Squire Patton Boggs’ Data Privacy and Cybersecurity practice, on the upcoming European Union General Data Protection Regulation (GDPR) compliance deadline.

PAGE 28

200,000

The number of people who had left Puerto Rico due to damage caused by Hurricane Maria, as of January 2018.

PAGE 21

“IT’S LIKE A TRUCK FAST APPROACHING US.”

Ann LaFrance, partner and coleader of Squire Patton Boggs’ Data Privacy and Cybersecurity practice, on the upcoming European Union General Data Protection Regulation (GDPR) compliance deadline.

PAGE 28

200,000

The number of people who had left Puerto Rico due to damage caused by Hurricane Maria, as of January 2018.

PAGE 21

“IT’S LIKE A TRUCK FAST APPROACHING US.”

Ann LaFrance, partner and coleader of Squire Patton Boggs’ Data Privacy and Cybersecurity practice, on the upcoming European Union General Data Protection Regulation (GDPR) compliance deadline.

PAGE 28

200,000

The number of people who had left Puerto Rico due to damage caused by Hurricane Maria, as of January 2018.

PAGE 21

“IT’S LIKE A TRUCK FAST APPROACHING US.”

Ann LaFrance, partner and coleader of Squire Patton Boggs’ Data Privacy and Cybersecurity practice, on the upcoming European Union General Data Protection Regulation (GDPR) compliance deadline.

PAGE 28

200,000

The number of people who had left Puerto Rico due to damage caused by Hurricane Maria, as of January 2018.

PAGE 21

“IT’S LIKE A TRUCK FAST APPROACHING US.”

Ann LaFrance, partner and coleader of Squire Patton Boggs’ Data Privacy and Cybersecurity practice, on the upcoming European Union General Data Protection Regulation (GDPR) compliance deadline.

PAGE 28

200,000

The number of people who had left Puerto Rico due to damage caused by Hurricane Maria, as of January 2018.

PAGE 21

“IT’S LIKE A TRUCK FAST APPROACHING US.”

Ann LaFrance, partner and coleader of Squire Patton Boggs’ Data Privacy and Cybersecurity practice, on the upcoming European Union General Data Protection Regulation (GDPR) compliance deadline.

PAGE 28
ACHIEVE EXTRAORDINARY

SEE THE POSSIBILITIES
It’s more than security, it’s business intelligence.

For product info #3 securitymgmt.hotims.com

Actual Hikvision customer
Jacob Burke
USA Alarm Systems, Inc.
FAIR & NEUTRAL:
Conducting Sexual Misconduct Investigations

Sexual harassment allegations keep coming, and employers must be prepared to conduct a fair, neutral, and effective investigation if a complaint is made in their workplace.

By Steven C. Millwee, CPP
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.
10 LETTERS

12 SECURITY MANAGEMENT ONLINE

14 EDITOR’S NOTE
Is timing everything?

20 NATIONAL SECURITY
Experts discuss a new power grid for hurricane-ravaged Puerto Rico. By Lilly Chapa

24 CASE STUDY
Drones help access fires. By Holly Gilbert Stowell

28 CYBERSECURITY
Will companies be ready to comply with European data privacy rules? By Megan Gates

56 ASIS NEWS
Volunteer leaders gather, and certification is streamlined.

57 ASIS BOARD OF DIRECTORS

60 LEGAL REPORT
A judge rules against botnet developers, and U.S. regulations on drug testing. By Megan Gates

64 INDUSTRY NEWS
A guard booth design competition is held. By Flora Szatkowski

68 MARKETPLACE

69 ADVERTISER INDEX

70 THE LIST
Anthony McGinty, CPP, discusses aviation security.
A COVER CONTROVERSY

SINCE I JOINED the editorial team at Security Management in 1993, I’ve seen and heard hundreds, if not thousands, of comments about the magazine: complimentary, critical, delighted, angry. You name it. Some readers had a visceral reaction to the January 2018 cover story by Michael Dorn on active assailant training in schools. The cover of that issue read “Run. Hide. Don’t Fight.” The cover offended some readers who assumed that Security Management was advising victims of active shooter events not to fight. This is not the case. At the urging of some of those upset by the cover, I will address how the editorial decision was made.

In its July 2016 issue, Security Management published a well-received article titled “Hide. Hide. Hide.” In the article, hospital security expert Michael D’Angelo, CPP, discussed his adoption of an active shooter protocol that his team calls “Cease to Exist,” which revolves around the “hide” part of the Run. Hide. Fight. protocol—and also comports with the “hide” aspect of the Run, Hide, Tell protocol developed by the U.K. Counter-terrorism Police in 2017. Hospital employees are taught to lock the doors, turn off the lights, silence any unnecessary machinery, and shelter in place until the police arrive.

This discussion of tailoring active shooter protocols to various workplaces and scenarios was further explored in the January 2018 cover story, which reveals the results of a study of Run. Hide. Fight. training for nonsecurity employees in 1,000 K-12 schools. When testing the employees on the protocol, researchers found that the employees applied the “fight” portion of the training first in many circumstances, not as the last option as designated by the protocol developed by the U.S. Department of Homeland Security (DHS) and the City of Houston in 2012. The article encouraged security professionals to ensure through testing, and retraining if necessary, that the message of the protocol was truly understood by nonsecurity employees.

Security Management has long been highly regarded by the security profession as a platform for knowledge and learning; never a forum for mandating policies or procedures—a near impossibility given the global nature of our membership. We regret that some readers felt that we were broadly calling for the abandonment of the Run. Hide. Fight. model.

Along with ASIS International, Security Management will be working with security experts, including those on the ASIS School Safety and Security Council, to devise a series of articles, webinars, and podcasts, along with other educational materials, to help security professionals prepare for, respond to, and recover from active assailant events.

Security Management will work closely with security professionals around the world to cover the issues most vital to our members.

Sincerely,

TERESA ANDERSON
VICE PRESIDENT EDITORIAL SERVICES
Editor-in-Chief, Security Management
LETTER TO THE EDITOR

I AM WRITING this letter on behalf of the members of the ASIS International School Safety and Security Council. Many of our members were concerned about an article appearing in the January 2018 issue of Security Management magazine, “Put Training to the Test,” written by Michael Dorn, and most especially, took issue with the cover of the magazine entitled, “Run. Hide. Don’t Fight.”

As one member states, “that concept alone is cringe worthy and is counter to the current widely used DHS concept of Run. Hide. Fight. One word, just one word, can alter people’s perceptions and our reactions. To allow something to be front cover that counters widely accepted policy shows a lack of internal communications and command of the subject.” Another member’s reaction to the cover was that “on the cover is a statement that is more than shameful, and crosses the line into the territory of gross professional and ethical negligence.”

Members of the council are worried that “the article could steer people in the wrong direction, or worse yet, create confusion and prevent schools from moving forward with an active shooter program.” Further, “telling people not to fight encourages the mentality that law enforcement will arrive quickly, engage quickly, and do all of the fighting on our behalf.”

A council member also voiced concern that “unfortunately, those not as experienced in this (the active shooter response) arena may well take this as gospel based on nothing other than the implied support of ASIS International that comes with publication in Security Management.”

“If any publication should ‘get it right,’ i.e. accurate, fair, and thorough, Security Management should be the trusted industry standard for school safety and security.” The bottom line for many of the experts on the School Safety and Security Council is that “we all need to be on the same page, chapter, and verse on a united front so that best practices are not countered even with the best of intentions.”

The article pointed out that the most dramatic feature of training “Fight” was used inappropriately, including in non-active assailant situations. This clearly points out some limitations of training and should cause those of us involved in training to thoughtfully consider how we train, as well as the need for refreshing and reinforcing the principles to ensure they are properly applied, especially when split-second decisions need to be made.

We all recognize that there was no malicious intent on the part of Security Management to convey information that could be construed as misleading or against industry standard. Rather, the publication of the article was intended to present another viewpoint from the traditional Run. Hide. Fight. training advocated by other security professionals. However, it is important to consider that “each individual has to make a decision when faced with (an active shooter) situation, and sometimes, fight may be the best option.”

Sincerely,

KEVIN DAVIS, J.D., CPP
VICE CHAIR
School Safety and Security Council

Tell us how we are doing?

Letters to the editor are welcomed and encouraged on all matters pertinent to security professionals. Letters should be emailed to teresa.anderson@asisonline.org.

Submissions may be edited for length and clarity.
EUROPEAN UNION DATA RULES

New EU data protection rules are set to go into effect in May 2018. The General Data Protection Regulation (GDPR) is designed to give citizens control of their personal data, according to the European Parliament. Many businesses wrongly assume that the GDPR does not apply to them because they’re not based in Europe. Others may not understand the scope of GDPR and are struggling to become compliant. The International Association of Privacy Professionals says that the global 500 will spend $7.8 billion on GDPR compliance out of a combined annual revenue of $26 trillion. Learn more via SM Online.

TASERS
In a December 2017 article, Reuters identified 104 cases of prisoners who died after being shocked with Tasers.

TRANSACTION FRAUD
Two-thirds of U.S. companies report an increase in fraud attempts over the past 12 months, according to a study issued by IDology, an Atlanta-based identity verification firm. The Fifth Annual Fraud Report: A New Landscape Emerges says that first-party fraud grew the most.

FIRE PROTECTION
An October 2017 report from the National Fire Protection Association breaks down the total cost of fire damage in the United States.

HARASSMENT RESOURCES
ASIS International and SHRM, an organization for HR professionals, offer resources for preventing harassment and conducting investigations.

DISASTERS
The United States has experienced 219 natural disasters since 1980 that reached or exceeded $1 billion in damage costs, according to a new analysis by the National Oceanic and Atmospheric Administration’s National Centers for Environmental Information.

CORPORATE FRAUD
Former Volkswagen executive Oliver Schmidt was sentenced to the maximum prison term of seven years and fined $400,000 for his role in the car manufacturer’s emissions scandal.

DATA BREACHES
U.S. Senator Bill Nelson (D-FL) introduced a bill that would require companies to disclose data breaches within 30 days of becoming aware of the breach.

ONLINE HARASSMENT
What constitutes online harassment? And when should social media platforms intervene? The Pew Research Center found Americans to be divided over these questions.

GO TO SM ONLINE FOR THESE AND OTHER LINKS MENTIONED THROUGHOUT THIS ISSUE.
Managing Change for Security Success

Join CSOs, key policymakers, and recognized thought leaders for strategic-level discussions, executive development, and high-level networking opportunities.

Explore the key drivers of change worldwide and their impact on your business

Get research-based leadership insights and business coaching

Go behind-the-scenes at the U.S. Bank Stadium, home of Super Bowl LII

You will walk away with deeper personal and professional relationships, as well as the knowledge to enable change—not just respond to it. You won’t want to miss it!

Learn more and register at asisonline.org/CSOSummit.

This event is open only to CSO Center members and those eligible for membership.
“Afternoons are the Bermuda Triangles of our days.” So writes Daniel Pink in his new book *When: The Scientific Secrets of Perfect Timing*. According to research, a dip in energy and cognitive awareness that Pink calls a “trough” affects human performance in profound ways.

A decline in vigilance in the afternoon is especially obvious in the medical field. Anesthesiologists are four times more likely to make a mistake at 3 p.m. than they are at 9 a.m. Gastroenterologists discover 5 percent fewer polyps during afternoon colonoscopies. The rate of hand-washing among nurses declines by 38 percent as the day wears on.

This phenomenon also reaches into the classroom—students taking standardized tests in the afternoon do significantly worse than morning testakers; the courtroom—judges are less likely to grant parole in the afternoon; and the boardroom—quarterly earnings reports are perceived more negatively in the afternoon, regardless of the information being reported.

This is because, explains Pink, most humans are governed by an internal clock, in which performance, happiness, and energy peak in mid-morning around 11 a.m., plummet around 3 p.m., and rise again around 8 p.m. This pattern repeats across days, years, and even lifetimes—people report lowest happiness in their late 40s.

However, Pink stresses that there is a simple way to boost performance and avoid these consequences. By simply taking a break, refocusing attention, or going for a walk, many of these negative outcomes can be mitigated.

Timing is not limited to individuals. Synchronizing timing in groups leads to both organizational success and personal happiness. The hearts of chorus members, notes Pink, synchronize during performances.

Connecting people to their environment and each other depends on external timing cues as well as interpersonal relationships. These cues are critical to success in the workplace.

“Certain activities—product development or marketing—establish their own tempos. But those rhythms necessarily must synchronize with the external rhythms of organizational life—fiscal years, sales cycles, even the age of the company or the stage of people’s careers,” Pink writes.

Internal and external cues point to good timing for *Security Management’s* latest venture. Along with this issue of the magazine, readers will find *Security Technology*, a supplement dedicated to providing news, case studies, and thought leadership around the latest in security technology.

The success of this quarterly supplement will rely on synchronization with security experts and technology leaders. As technology increasingly governs our personal and organizational futures, the time has come to share your experiences and give us your feedback. What technology stories do you want to tell? What issues do you want to learn more about? By synchronizing our efforts, we create a better outcome for everyone.
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.COM/BLUR

LISTEN • DESIGN • BUILD • SUPPORT

For product info #6 securitymgmt.hotims.com
They are as skilled in committing these frauds as any skilled person is in any field of endeavor,” says Alan Brill, a director with Kroll’s cybersecurity and investigations practice. “They are criminals, but you have to respect the level of skill that they have, to know what you are up against.”

This fraudulent activity is affecting more and more companies, according to a new study. About two-thirds of U.S. companies reported an increase in fraud attempts over the past 12 months, according to The Fifth Annual Fraud Report: A New Landscape Emerges, a study issued by IDology, an Atlanta-based identity verification firm. Last year, fewer than half (42 percent) of U.S. companies reported such a rise.

Fraud is thriving these days, and many of its practitioners have acquired daunting levels of skill and ingenuity for reading the current operational environment, finding weak links, and adjusting their methods to maximize the likelihood of successful scams, experts say.

“The biggest challenge faced by businesses in the fight against fraud has been the continually shifting tactics used by fraudsters,” reads the study, which finds that 71 percent of organizations cite “shifting fraud tactics” as their greatest challenge.

Use of fraudulent credit, debit, and prepaid cards is still the most prevalent type, with 65 percent of respondents saying that it is the most common method in their industry. However, there are signs that it is starting to decrease. That 65 percent figure is actually down from the 73 percent of respondents who cited that fraud type in last year’s survey.

According to the report, the reason behind this decrease is the
widespread adoption of EMV chip cards, which have reduced point-of-sale fraud. With chips making it harder to commit this type of fraud, more criminals are shifting to an online environment, where the customer is not present. “They will try to find the path of least resistance,” IDology CEO John Dancu says.

There’s another driving factor behind the shifts in the fraud landscape, and it has to do with how nimbly the fraudsters share knowledge. “They are really good at communicating among themselves,” Dancu says. Sometimes, they will discuss methods on the Dark Web; this keeps them situationally aware and helps them change methods if necessary.

Some are also not shy with expressing pride of craft. “When they find a weak link, they are happy to tell everybody else about it,” Dancu explains. “If you’re on the Dark Web or their other forums, you can see the interactions and the professional enjoyment that they have in letting other people know what they have discovered. It’s about being The Man.”

Those dark websites and other places where fraudsters sell information and data are pretty sophisticated enterprises, Brill says. “There is a comradeship among people who do this. They do meet at the marketplaces, and these marketplaces don’t look that different from eBay, with vendors getting rated by people that buy from them,” he explains. Some vendors even offer BOGO specials, he adds.

As is true with most fields of endeavor, this increased professionalization brings about more specialization. So, some fraudsters specialize in malware, some in the monetization or selling of breached data, and some in “social engineering”—knowing how to get to the right entry point to access information, Brill explains.

He offered the following example of a social engineering specialist. These days, many banks frequently advertise how effective they are in protecting customers against fraud. In this environment, it may then be no surprise if one day you get a phone call from Visa security, with the caller informing you that your card was just charged with suspicious activity—$300 from an adults-only emporium in Las Vegas. Horrified, you deny the charge and ask for it to be cancelled, and so you gladly give your card information, Social Security number, and date of birth when the caller asks if they can verify you as the cardholder.

But what you might not realize is that you just handed over your information to a criminal posing as security. This type of thief takes advantage of the expectations created by frequent bank commercials that promote their quick security operations. “In effect, you have been primed for a social engineering hit,” Brill says.

Although the study finds that customer-present credit card fraud may be decreasing, it also finds that synthetic identity fraud (SIF) is a growing problem. In an SIF scam, a combination of real and fabricated identity information is often used to create a new identity. Thirty-one percent of businesses in the report say SIF has increased, and 58 percent are “extremely” or “very” worried about it. Helping to drive this problem is the recent flood of major data breaches, which gives criminals more identity data to use.

In Kroll’s investigations practice, Brill is seeing a big increase in the following type of case. A fraudster obtains the Social Security number of a young child in the aftermath of a data breach, then uses it with other information to open a few credit accounts, including one or more credit cards.

The scammer then exploits the accounts for years, with charges that are never repaid and lapse into default. Finally, the young child becomes old enough to apply for a credit card, or a lease on an apartment, and is surprised to find out that his or her credit rating is abysmal.

ONLINE HARASSMENT

In two vignettes, respondents were asked if and when social media platforms should step in and take action to stop events involving harassment. Individuals were more likely to respond that platforms should act when a threat was directed at a female.

Social media should intervene on threatening messages to males vs. females

67% 76%

SUPPLY CHAIN SECURITY

BY DARREN J. PROKOP. Butterworth-Heinemann; Elsevier.com; 200 pages; $49.95.

ANYONE WHO intends to enter the realm of supply chains and logistics must read Global Supply Chain Security and Management. Author Darren Prokop brings vast experience in the academic and practical worlds of supply chain management to this book. He goes the extra mile to package a tremendous amount of critical information in a compact volume to produce an easy-to-read narrative and valuable reference guide to these types of global operations.

Not only does the book identify the threats of today and tomorrow, it also provides useful insight on how to combat them. Going beyond the issues of insider/outside theft and shipping damage, Prokop redefines the threat to include terrorism and natural disasters. He adds key chapters on topics of human and natural threats, information technology, and risk mitigation.

Prokop introduces the concept of game theory in the synergies between players in the global shipping arena, and he explains how a competitive situation may morph into a cooperative one. He points out the dual role that government plays in the global shipping effort—serving as both a policing agent and a supply chain partner. Key takeaways include recent U.S. regulatory decisions, the latest technologies for securing infrastructures, and up-to-date theories and techniques of industrial organization and security.

This book is an excellent tool for faculty and students of security management and supply chain management. Security practitioners in other disciplines would do well to add it to their professional libraries, as well.

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.

Marcus Christian, an attorney in Mayer Brown’s White Collar Defense & Compliance group, also sees SIF as an increasing problem. Christian, a former prosecutor in the U.S. Attorney’s Office for the Southern District of Florida, has heard reports that some of the criminal organizations in South Florida have been shifting away from selling narcotics and toward identity scams. “The money is as good as, if not better than, the drug trade,” he says. In addition, it is often perceived as a less dangerous practice, and through connections in local school systems and banks, these criminals can obtain stolen data, he adds.

The second-most cited type of fraud in the report—first-party or friendly fraud—is also on the rise, with 51 percent of respondents saying they have been a victim of it, nearly double the percentage (26 percent) of respondents who cited it in last year’s survey.

First-party or friendly fraud generally describes fraud committed by individuals using their own accounts. These types of fraudsters might make an online purchase and then dispute the charge after the merchandise has been received, or they might open credit card accounts with the intention of maximizing charges and then lapsing into default to avoid full repayment.

One reason first-party fraud is increasing, the study finds, is that it is difficult to foil; it is hard to disprove false claims that ordered merchandise was never received, for example. However, experts say that big data applications hold some potential in this area as a security tool, because they can be used to recognize patterns of excessive refund requests and other telling information.

Finally, Dorcu says that another cause for optimism in the fight against fraud is that an increasing number of companies are realizing the importance of working together. Fraud is a serious issue for companies regardless of industry, and since the perpetrators are sharing information and strategies, those fighting fraud need to do the same, under a consortium mindset.

“Getting connected and talking with peers is really an important part of solving the problem,” Dorcu says. “Be flexible, be collaborative, and be open-minded to what’s going on out there.”

TASERS AND THE UNITED NATIONS

TASER USE is once again in the news. Nils Melzer, the special rapporteur on torture for the United Nations (U.N.) Commission on Human Rights, called for U.S. officials to investigate Taser use on inmates in jails in Ohio, Tennessee, Oklahoma, and Arkansas.

Melzer made his remarks after reviewing footage of 22 incidents in jails in Franklin County, Ohio; Cheatham County, Tennessee; Franklin County, Arkansas; and McCurtain County, Oklahoma. The footage was obtained to the fraud report.

Visit SM Online for a copy of the fraud report.

PHOTO BY THINKSTOCK
which violated the United Nations’ prohibition on cruel and inhuman punishment. In some cases Taser use amounted to torture.

In its video report and article published in December, Reuters identified 104 cases of prisoners who died after being shocked with Tasers. Nearly 80 percent of those 104 inmates had not been convicted of a crime. Reuters was able to gather significant detail on 70 of the 104 cases; in more than two-thirds of the 70, the inmate was already immobilized—pinned to the ground or held by officers—when shocked. About one-third were cuffed or in other restraints.

Of those 104 cases, Reuters was able to obtain cause-of-death information on 84 cases. The Taser was identified as a contributing factor of death in more than 21 of those 84 cases.

Jens Modvig, chairman of the U.N. Committee against Torture, also said the incidents published by Reuters represented blatant abuse that may violate laws. The United States, as a signatory to the U.N. Convention against Torture, is obligated to investigate the cases, Modvig argued.

The Reuters report and the statement by U.N. officials marks the latest chapter in the ongoing debate on Taser use.

Various studies have shown that Tasers may pose some health risks, depending on how they are used, and on whom.

But other studies show they can be used as an effective enforcement tool in some cases, that may ultimately reduce the number of violent assaults and sometimes even save lives. The U.N.’s Melzer, while condemning the incidents published by Reuters, also said that in general Tasers can be a justifiable tool for prison guards as an alternative to a gun, to incapacitate a person who poses a threat.

And this year may see the San Francisco Police Department adopt the use of Tasers. It is one of the last major U.S. forces to do so. In November 2017, the San Francisco Police Commission voted 4–3 to allow the city’s police department to begin equipping its officers with Tasers in December 2018. The vote was taken near the end of a long meeting that was interrupted by a protest that led to a lockdown of City Hall. The issue had been debated and rejected in the city for years.

---

**Tasers may pose some health risks, depending on how they are used, and on whom.**

---

**CEIA Metal Detectors for Campus Protection**

PD240 Hand-Held Detector

HI-PE Plus WTMD

**THE CEIA DIFFERENCE**

- The standard for safety, convenience and accuracy
- Superior detection and throughput
- Exceptionally high discrimination of non-threat items
- Compliant with the strictest security standards
- Unmatched reliability
- Walk-through, hand-held and table-top models to fit facility needs

security@ceia-usa.com 888-532-2342

WWW.CEIA-USA.COM

For product info #7 securitymgmt.hotims.com
NATIONAL SECURITY | INFRASTRUCTURE

Lilo Pozzo, an associate professor of chemical engineering at the University of Washington, traveled to Jayuya, Puerto Rico, in November with a group of students to assess the impact of extended power outages on public health. Due to its remote, mountainous location, the municipality was still largely without power, and Pozzo’s group found that people with respiratory problems were greatly impacted.

“The overall message was that the people with respiratory ailments were in the worst condition because they weren’t necessarily evacuated like patients that had more evident health problems, so these people with chronic conditions essentially stayed behind, and they are suffering because they can’t power their devices to run therapies,” Pozzo explains.

FOR THE CITIZENS of Jayuya, Puerto Rico, December 15 came and went without fanfare—and in the dark. The U.S. territory’s governor, Ricardo Rosselló, had estimated that 95 percent of Puerto Rico would have power back by mid-December following the devastation brought by Hurricane Maria in September. As of press time, that estimate had been extended to February.

Lilo Pozzo, an associate professor of chemical engineering at the University of Washington, traveled to Jayuya, Puerto Rico, in November with a group of students to assess the impact of extended power outages on public health. Due to its remote, mountainous location, the municipality was still largely without power, and Pozzo’s group found that people with respiratory problems were greatly impacted.

She describes people who are unable to operate their sleep apnea machines or administer asthma treatments. Those who need oxygen now have to wait for tanks to be delivered to the municipality because their standalone oxygen machines could not be charged. The main clinic in town had borrowed a generator after its first one broke down, but can only provide essential services due to concerns of damaging the current generator. All vaccinations and refrigerated medications were spoiled, and citizens with mobility issues or sensitive diets have also been affected.

The city’s two major factories have also continued to operate by running generators, which Pozzo says is expensive and inefficient. The towns-
Puerto Rico’s power system was in trouble long before Hurricane Maria hit.

People are fearful that it will be difficult for the factories to continue operations if conditions don’t improve quickly or if extended power outages following natural disasters become the norm. “If you get hurricanes every year, that’s going to change their economic calculations and could potentially create loss of workforce,” Pozzo notes.

Despite the dire situations in part of Puerto Rico, power restoration has been slow due to a process fraught with politics and finger pointing between the territory’s leaders and the U.S. federal government about the amount of aid that should be provided. However, Puerto Rico’s power system was in trouble long before Hurricane Maria hit.

In the days following the territory’s brush with Hurricane Irma in early September, which briefly knocked out power for a million people, investors became more vocal about privatizing the territory’s struggling power grid. The Puerto Rico Electric Power Authority (PREPA), the largest public utility in the United States, had declared bankruptcy in July, and what little maintenance it was conducting on the island’s power grid fizzled. Politicians, energy experts, and other stakeholders acknowledged that the grid might not hold up much longer without serious changes.

And then, two weeks later, Hurricane Maria made landfall in Puerto Rico as a Category 4 storm.

The entire island lost power. Several neighborhoods were destroyed. Most communication networks across the island were crippled. Fresh food and potable water became scarce. The official death toll in Puerto Rico is 64, but estimates suggest more than 1,000 people may have died from the storm and its aftermath. As of early January, 43 percent of the island still had no power, and more than 200,000 citizens have left their darkened communities for the continental United States.

“Puerto Rico is being supported to a large degree by U.S. power companies right now, but that’s not sustainable,” explains Mark Weatherford, chief cybersecurity strategist at vArmour. “That’s why there needs to be a long-term plan here, but it’s going to cost money. This is going to be a test of our nation in what we’re willing to support to rebuild a state that was already teetering on bankruptcy.”

When Hurricanes Harvey and Irma struck Texas and Florida last fall, power crews and equipment rolled in from other U.S. states to get the affected regions up and running. But the sheer magnitude of Hurricane Maria’s damage to Puerto Rico—and its island location—made it difficult for other U.S. utility companies to lend a hand, says Daniel Kirschen, an engineering professor at the University of Washington and a member of the Clean Energy Institute.

“Typically, utilities are eager to help each other in those situations because of the mindset that this time it’s your turn, but the next time it might be mine,” Kirschen says. “So these companies are usually very willing to lend crews for repairs. Now, of course, Puerto Rico is an island so it’s harder to organize sending crews down there, which on top of all the other problems has made recovery more difficult.”

Brian Harrell, CPP, the vice president of security at AlertEnterprise and former director of critical infrastructure protection at the North American Electric Reliability Corporation (NERC), details what is involved in sending crews to repair Puerto Rico’s power grid. Workers and tools must be flown to the island, and heavy equipment such as bucket trucks, transformers, and wires must be transported on ships, which makes the logistics of recovery difficult. Upon arrival, crews must manage downed lines, clear debris from roads, and fully repair the system, he says.

“When the aftermath of such devastation, it is imperative that safety and security is established on the ground,” Harrell says. “Before critical infrastructure can be repaired and restored, it’s vital that line crews, aid workers, and emergency personnel feel safe while conducting their jobs.”

But as each power line is restrung to bring electricity back to the island, experts are pointing out the opportunity to build a more resilient, smarter power grid that will prevent future catastrophic damage to Puerto Rico’s infrastructure—but nobody has come up with a plan.

CLIMATE DISASTERS

Sixteen separate disasters, from severe storms to drought, incurred damages of at least $1 billion each in the United States in 2017. Hurricane Harvey was the costliest disaster, at an estimated $125 billion. Together, Hurricanes Harvey, Irma, and Maria were responsible for $265 billion in damages and 251 deaths.

U.S. natural disasters in 2017 cost

$306.2B

“Given the complete destruction of the island’s power system, an opportunity has also presented itself to modernize the way electricity is generated, along with how it can be efficiently transmitted with newer technology,” Harrell adds. “A key to preventing this type of destruction from ever happening again will be to build resilience and redundancy into the system.”

Stuart McCafferty, president and CEO of GridIntelect and a National Institute of Standards and Technology (NIST) community resilience fellow for electrical power infrastructure, says that Puerto Rico needs to move beyond its reliance on fossil fuels, which are expensive and unsustainable. McCafferty has been involved in the U.S. smart grid initiative since the beginning, creating the first smart grid maturity model for the U.S. Department of Energy (DOE) and a tool to evaluate a grid’s resiliency. He says that while continental U.S. energy providers and government officials embraced the shift towards a smarter grid, there was a disconnect when it came to waterlocked states and territories. Hawaii has paved its own way by working with DOE to develop an unprecedented clean energy initiative in 2008—drawing the majority of the state’s energy from renewable resources. Puerto Rico had made no effort to update its infrastructure.

Despite the critical situation in Puerto Rico right now, McCafferty says that the territory has an “incredible opportunity” to build localized power grids that are self-reliant and will not allow downed transmission lines to knock out power for the entire island.

Weatherford agrees. “With an aging infrastructure like that, unfortunately the only thing they will be able to do is rebuild from ground zero,” he says. “They need to start over, and the good news is this gives them the opportunity to build a 21st century infrastructure—but it’s going to cost a lot of money to do that.”

Although PREPA is cash-strapped, McCafferty says money can come from federal grants and labs, venture capital, angel investors, and self-funded corporations. However, a sorely-needed roadmap for the territory’s power grid is nowhere in sight, even as legacy infrastructure is being repaired.

“I don’t see anyone coming up with any real solutions because of the financial issues and mismanagement of the grid by the operator,” McCafferty explains. “Puerto Rico needs a roadmap, and it doesn’t even have to be based on any of the financial needs. Once you’ve got that laid out, then you can start prioritizing and identifying the funding mechanisms to make that happen.”

Weatherford suggests setting up temporary generators and small microgrids to keep the lights on for citizens while officials go back to the drawing board to figure out a more resilient solution. “Use temporary money to keep the lights on, and use long-term capital to rebuild the infrastructure,” he says. A robust microgrid system, which would keep power outages isolated, paired with renewable energy such as solar and wind power, would be an ideal setup, he says.

Kirschen, who studies how to effectively deploy repair crews to restore critical infrastructure, agrees that redesigning the grid is not going to happen overnight, and crews need to focus on rebuilding what they can of the existing infrastructure.
“We’re not at a point where we can generate quite enough power with solar generation to satisfy all the island’s needs,” Kirschen says. “What I see is a combination of a traditional grid built to a higher standard so it can withstand hurricanes and other disasters, combined with local microgrids designed to survive these hurricanes, so that if the main grid is broken for a while, you can still meet the emergency medical and essential needs until the main grid is repaired. It’s particularly important in Puerto Rico because the landscape is rugged and there are some really remote areas that are hard to reach. Therefore repairing the grids to reach those areas will take time, so having one of those small emergency microgrids can be extremely useful.”

Pozzo says that a solution for remote areas like Jayuya that would provide critical services during an emergency would be ideal. “You’re not restoring power to everybody, but you’re at the very least able to maintain the critical needs, storing medicine, providing power to people with medical devices,” she says. “I believe that if the town had distributed independent systems—it could be clean energy but could also run on generators that are larger and more effective—they would fare much better, just because they could focus on repairs in a more localized way.

Part of Pozzo’s research in Jayuya was quantifying exactly how much energy it would take to meet the critical needs of the entire community to better prepare emergency shelters to handle future power outages.

“We’re analyzing ideas where you could invest in providing power to schools that could serve as shelters, so you need to understand how patients are distributed in a community and whether they are able to get to the shelters to have their needs met and how much energy would be necessary to satisfy the number of patients that would go there,” she explains. The academic paper on her team’s findings will be published in the spring.

“Climate change is happening—we’re going to get natural disasters more frequently and more severely, so we have to make sure that our infrastructure is built to a standard that is appropriate for these natural disasters,” Kirschen says. 

---

**CRITICAL INFRASTRUCTURE PROTECTION (CIP)**

**ABLOY SECURITY**

An ASSA ABLOY Group Brand

1 800-367-4598

In Canada 800-465-5761

Fax 972-753-0792

E-mail info@abloyusa.com

Website www.abloyusa.com

For product info #8 securitymgmt.hotims.com
This aerial view over city buildings sparked an idea for the department: what if it could have similar drone video during every fire it responded to—as the fire was being fought?

“The incident commander is on the ground like a general calling all the shots. He’s got people in the building doing searches. He’s got people on the roof. He’s the guy making decisions with the most information,” says Tim Herlocker, former director of the FDNY Emergency Operations Center. Enhancing that commander’s situational awareness with a drone would allow him to safely navigate a team of firefighters in and around the fire, especially on those hard-to-see rooftops.

When a fire strikes in the middle of the night, “some of our most senior chiefs have to start making decisions—’Do I have to go to the fire? Do I have to respond back to our headquarters?’” Herlocker notes. “And being able to actually see what it looks like—the color of the smoke, the volume of the smoke, the flames, whether they’re trying to save it from moving to an adjacent building—all those things require experience honed over years as a firefighter.”

The FDNY had been streaming helicopter video to the incident commanders for a number of years under contract with the New York Police Department and local news stations. “All of the options were good, but as technology progressed, we knew that we needed constant, persistent aerial surveillance of fire events,” Herlocker says. Drones would provide much more flexibility, like the ability to hover directly over a fire or focus on a particular part of the blaze.

With the proliferation of drones, obtaining the right unmanned aerial vehicle was possible, but the department ran into another obstacle. “About 65 percent of the airspace in New York City is what’s called Class B airspace,” Herlocker explains, “and
it’s the most restricted airspace in the country.” Under federal airspace rules, the U.S. Federal Aviation Administration (FAA) does not allow drones to fly within five nautical miles of any U.S. airport. New York City is within that range of three major airports: LaGuardia Airport, J.F.K. International Airport, and Newark Liberty International Airport.

Because of FAA rules, “we realized the program wasn’t going to work, so we shelved it,” he says. However, about six months later, the department approached the FAA with a new idea. “We went back to the FAA, and we said, ‘We need to fly in your restricted airspace and we need to do it day and night on short notice, but we’re going to mitigate the threat to your airspace by tethering our drones to the ground,’” he says.

The FAA agreed to the idea, and the FDNY began looking for a vendor that could meet its technological requirements. “We went searching for technology. We had a rough idea of what we wanted. There truly are only a handful of vendors that do purpose-built tethered devices,” he says.

The FDNY wanted a unit that was not only tethered by a thin cord to a power source on the ground, but that could deliver instantaneous, high-definition or infrared video.

Most battery-operated drones are too lightweight to remain in flight for longer than a few minutes, so the tether would be a continuous power source. This would allow the drone to hover for hours on end. The FDNY also wanted the drone to remain directly over the anchor port where the drone takes off, but without using GPS. In an urban environment like New York City, metal structures and magnetic fields can throw off the vehicle’s navigation system. “GPS signals can bounce off buildings, and the drone can chase a [wrong] signal and get out of position—so it’s a tough environment to fly in,” Herlocker says.

The FDNY selected Hoverfly Technologies of Orlando, Florida, which provided an eight-pound drone with a thin tether cord. The department began a pilot phase of the program, which lasted six months. “We’ve done a lot of testing, we’ve made a ton of mistakes, we’ve corrected technology,” he says. The program began flying missions in March of 2017, and had flown 26 fires as of December 2017.

The department currently has three drones, which are deployed for second alarm or greater fires (the number of alarms indicating the severity of the fire). Video of the fire from the drone’s HD and infrared cameras is streamed to the incident commander and other senior leaders in the department via a video recording network. The users...
receive the video directly to their smart devices by clicking on an encrypted link sent from Amazon’s cloud.

FDNY firefighters who show interest or have a background in drones are trained as pilots. “We put them through an online training session that teaches the FAA standards, then at some point, when they have enough time on the device under supervision, we certify them.” While it doesn't take much technical skill to pilot the drones, Herlocker notes, it does take a sound sense of judgment. “You have to decide, is it safe to put the drone up, is there too much wind, are there too many overhead obstacles, or is the fire worth the risk of putting it up?” he notes.

The drone is used in each mission to keep firefighters away from danger, show first responders where to direct water hoses, help them create vents in the roofs of buildings, and more.

The drone also helps with ladder placement. In the spring of 2017, the department was fighting a five-alarm fire at a large apartment building. “The drone hovered in place for three hours at 130 feet. The firemen were using the drone to move ladders around and hit different hot spots on the roof,” with a precision that helicopter video would not have provided in the past, Herlocker explains.

Herlocker notes the department’s relationship with the FAA has also become an asset to fighting fires. The department is required to call and clear each drone flight in advance. Recently, the FDNY had to put through an emergency request when a fire was within one mile of LaGuardia airport. “We couldn’t even finish the sentence before the FAA operator said, ‘We were wondering what took you so long—you have permission to go.’”

In the future, the FDNY hopes to expand the drone program to include several vehicles with ready-to-deploy drones that nest on top. The department is also looking into free-flight drones to fly inside of burning buildings, with the ability to make tight turns and assist in rescue operations.

While Herlocker says it’s hard to measure exactly what the drone program has prevented, including injuries to firefighters and buildings from destruction, it has undoubtedly benefited the department. “We want the incident commander to have just a little bit better view to make safety calls and to fight the fire more efficiently,” he says.
We build security booths as strong as a tornado

In December of 1997, two security booths made by B.I.G. Enterprises stood in the pathway of Super Typhoon Paka in Guam. Though surrounding structures were flattened, the booths, including their glass windows, were intact after the 220 mph hurricane passed over.

Your perimeter security must stand-up to the strongest threats: bad guys or natural disasters.

At B.I.G., we bring a half-century of perimeter security insight to you. We know how to fabricate a booth with every modern security demand on the inside, but one that fiercely protects your people and facility on the outside. From the U.S. military to Disney, they come to us for value and unrelenting safety. Come visit the vast Gallery of Booths on our website. Let us build your image.
Such is the case with the upcoming European Union General Data Protection Regulation (GDPR) compliance deadline on May 25, 2018, when regulators will begin to issue fines to companies not abiding by the regulation’s vast new privacy and security requirements.

“It is like a truck fast approaching us,” says Ann LaFrance, partner and coleader of Squire Patton Boggs’ Data Privacy and Cybersecurity practice. “We’re getting an avalanche now of interest and requests for proposals, and clients are really now starting to focus on this. Why they waited till the last six months? Who knows. But at least they are now seriously starting to focus.”

The GDPR was first drafted in 2012 as part of the EU’s push for a Digital Single Market. The regulation lays out the rights EU citizens have in regard to their personal data and how data controllers and processors respect those rights. The regulation guarantees EU citizens the right to be forgotten, easier access to personal data, data portability, data breach requirements, data protection by design and default, and stronger enforcement of those requirements.

The EU Parliament approved the regulation in April 2016, and Jan Philipp Albrecht—who steered the legislation through—called it a victory for consumers and businesses alike. “The General Data Protection Regulation makes a high-uniform level of data protection throughout the EU a reality,” he said in a statement. “Citizens will be able to decide for themselves which personal information they want to share. The regulation will also create clarity...
AMICO
HIGH SECURITY PERIMETER SYSTEMS

AMIGARD - The World's Strongest Perimeter Security System
ANC - Non Conductive High Security Perimeter Solution

CHAMELEON - Upgrade Your Existing Chain Link Fence to a High Security Curtain Wall System for up to 40% Less Than New

Our Professional Team is Ready for your Next Project

855-552-6426
amicosecurity.com
amicosecurity@gibraltar1.com

SEE OUR ENTIRE LINE OF SECURITY FENCES ON DISPLAY IN BIRMINGHAM, AL - INSTALLATION TRAINING AVAILABLE

For product info #12 securitymgmt.hotims.com
Why they waited till the last six months? Who knows.

for businesses by establishing a single law across the EU. The new law creates confidence, legal certainty, and fairer competition.”

Organizations that conduct business in Europe were given a little more than two years to become compliant with the new regulation, before fines of up to 4 percent of global turnover kick in. During that window, the Article 29 Working Party—as well as other advisory bodies—have issued guidance about how to implement GDPR. On May 25, the working party will be succeeded by the European Data Protection Board (EDPB) to ensure that GDPR is consistently applied throughout the EU.

“To achieve this, the EDPB will be empowered to issue opinions or authorizations regarding a variety of matters, such as Binding Corporate Rules, certification criteria, and codes of conduct used by companies; to adopt binding decisions, especially to ensure consistency between supervisory authorities; and to issue opinions and guidance on relevant issues concerning the interpretation and application of the GDPR,” according to a fact sheet.

And while organizations have had two years to come into compliance, LaFrance says she is doubtful that most companies will be fully compliant by the deadline.

One reason is that many businesses may wrongly assume that the GDPR does not apply to them because they’re not based in Europe. Others, LaFrance says, do not understand the scope of GDPR and are struggling to become compliant.

“The problem is there’s cognitive dissonance about what GDPR is all about,” she explains. Non-EU based companies “think that it’s mainly about IT security, IT systems, and security around them, and in fact that’s only one piece of the overall pie.”

Instead, GDPR cuts to the heart of what those systems do—store and transfer data—and requires organizations to integrate privacy and security into their overall business processes. For instance, GDPR requires organizations to map their data and how it’s collected.

“This is a very expensive exercise these companies are going to have to go through, and they don’t really understand before they get started the breadth of the task ahead of them,” LaFrance says. “So, when they hire you and you start telling them this, there’s an ‘OMG’ moment.”

Because of these factors, LaFrance says some small businesses with less data might be compliant by the deadline, but most organizations will not be.

Companies will also have to reassess their third-party vendors to ensure agreements with them are GDPR compliant, which can be a time-consuming process.

“The normal company will have 20 or 30 outsourcing agreements,” LaFrance says. “And you’ve got to go through and renegotiate all of those agreements so that they are GDPR compliant. It’s a huge task. And it could be very expensive because the counter party might say, ‘Yeah, we’ll sign up for that but it’s going to cost you more.’”

And in fact, companies are expecting to spend billions on GDPR compliance over the next year, according to the International Association of Privacy Professionals (IAPP) Annual Privacy Governance Report.

The report—sponsored by Ernst & Young—surveys roughly 600 privacy professionals about their size of staff, priorities, and expenditures for the year. In the 2017 survey, IAPP Content Director Sam Pfeifle says respondents indicated that the global 500 will spend $7.8 billion on GDPR compliance out of a combined annual revenue of $26 trillion.

“It’s not a huge number—we’re not trying to say this is equivalent to Sarbanes Oxley,” Pfeifle says, but he adds that it is a massive increase from 2001 when IAPP was created and organizations were only spending millions on privacy.

“It wasn’t a thing unless you were in the healthcare space or in financial services,” he adds. And typically, these organizations had a small department that was compliance focused and working with development teams at the later stages of development.

“It was really just people bringing you something at the end of the product development lifecycle and asking: ‘Is this legal?’” he says. “You’d say, ‘Yeah, it’s legal.’ You’d check the box and off you’d go.”

**GDPR BASICS**

The EU General Data Protection Regulation is an extensive document that focuses on consumer rights, privacy, and cybersecurity. Below are some of its provisions.

1. The right to be forgotten
2. Requirement for “clear and affirmative consent” for private data collection
3. The right to transfer data to another service provider
4. The right to know when your data has been hacked
5. Privacy policies explained in clear and understandable language
6. Fines of up to 4 percent of global turnover for noncompliance

**FACT BOX**

**GDPR BASICS**

The EU General Data Protection Regulation is an extensive document that focuses on consumer rights, privacy, and cybersecurity. Below are some of its provisions.

1. The right to be forgotten
2. Requirement for “clear and affirmative consent” for private data collection
3. The right to transfer data to another service provider
4. The right to know when your data has been hacked
5. Privacy policies explained in clear and understandable language
6. Fines of up to 4 percent of global turnover for noncompliance

GDPR, on the other hand, requires that privacy and security be built into all business processes. To do this, companies are spending in a variety of ways, including adjusting the products and services they deliver.

For instance, Pfeifle gives an example of checking into a hotel and signing up for complimentary Wi-Fi. In the past, when guests would go through that process they would fill out a form that had a prechecked box indicating they wanted to receive promotional emails from the hotel. They would have to opt-out not to receive those emails.

“In the GDPR, you have privacy by default,” Pfeifle says. “Which means that you cannot precheck those boxes. So, someone is going to have to go and recode that page to make it so that box is not prechecked.”

For smaller companies, that could be a low spend, but for large corporations that are consumer facing—like Amazon—that could be vastly more expensive.

The other areas that organizations are spending on to become GDPR compliant include staffing, such as internal staff to conduct privacy impact assessments, and outside counsel and consultants that specialize in privacy and privacy management technology.

“We’re now seeing software packages that are specifically designed for managing privacy impact assessments—you can assign tasks, you can do reporting, you can have threat dashboards,” Pfeifle says. “A lot of them mimic security management software.”

These efforts are helping organizations move towards compliance, which is critical: only 40 percent of those surveyed by IAPP said they expected to be compliant with GDPR by the deadline.

“More important than being compliant is being able to demonstrate that you’re making the attempt,” Pfeifle says. “If a regulator showed up at your door and said, ‘Show us you are compliant with the GDPR,’ how would you do that? That’s what the GDPR asks you to do.”

LaFrance’s views mirror Pfeifle’s, because—in her opinion—regulators will be looking for organizations to make a good faith effort towards compliance.

“For the most part, if you’ve made a good faith effort to get a plan in place and you’ve taken the steps that you can between now and May to really get the ship moving in the right direction with a plan to sort things out by the end of the year, you’ll be given a good pat on the back by any regulator that is going to do a spot audit of your records,” she explains.

Some companies, however, might face more scrutiny after the deadline than others, such as those that are consumer facing and, if compromised, could create significant legal or economic consequences for consumers.

“I think they’ll also consider whether there have been complaints by individuals or if there have been a number of reported data breaches,” LaFrance says. “Regulators might look then to see if there have been lots of repeat offenders, and then go and do an audit. I imagine they will try to start with the obvious.”

The regulation lays out the rights EU citizens have in regard to their personal data and how data controllers and processors respect those rights.
Sexual harassment allegations keep coming, and employers must be prepared to conduct a fair, neutral, and effective investigation if a complaint is made in their workplace.
he recent flood of sexual harassment allegations in the United States, from Hollywood to Capitol Hill to New York City, has given people around the world new confidence to publicly denounce sexual harassment and other types of misconduct.

One powerful example is the Twitter hashtag, #MeToo, which has now been used by more than 1.7 million people in 85 countries to speak out and name their harassers. The allegations have resulted in tangible change: in the past several months dozens of public figures, accused of behaviors ranging from inappropriate harassment to sexual assault, have been fired or forced to resign from high-profile positions.

This remarkable spike in firings is also an extension of a longer-term development. Over the past five years, 5.3 percent of CEOs globally have been forcibly removed due to ethical lapses, including harassment, according to a PricewaterhouseCoopers study. In the United States, that’s a 102 percent increase from the previous five years. And during last year alone—before the
COVER STORY

BY STEVEN C. MILLWEE, CPP

#MeToo movement—harassment cost U.S. companies more than $160 million in U.S. Equal Employment Opportunity Commission (EEOC) settlements, an all-time high.

Some say these unprecedented developments represent nothing short of a social revolution, one that will have serious ramifications for employers.

After the news of allegations against Hollywood mogul Harvey Weinstein came out, the EEOC saw a fourfold increase in visitors to the sexual harassment section of its website. This trend demonstrates that employers must be prepared for the possibility that harassment complaints within their organizations may increase, and they must have effective policies and procedures for responding and acting on them.

When these accusations come out, many organizations are quick to end established relationships with the person being accused—usually to protect the enterprise and the brand, but also to show support for those reporting the allegations. However, it is important to remember that conducting a competent investigation to uncover the truth is vital. It protects the enterprise and all parties involved, and it will encourage other victims of misconduct to come forward.

This article explores how employers, employees, and those commissioned to investigate allegations of misconduct can develop proactive procedures to ensure that the rights of all parties are equally considered in every investigation. Establishing such informed procedures mitigates the risk of civil action, while demonstrating a commitment to fairness.

UNDERSTANDING THE OFFENSES

There are generally three classifications of sex-related incidents: harassment, sexual harassment, and sexual assault. The following is a breakdown of how the three are legally defined in the United States.

**Harassment.** Harassment is a form of employment discrimination that violates Title VII of the Civil Rights Act of 1964, the Age Discrimination in Employment Act of 1967 (ADEA), and the Americans with Disabilities Act of 1990 (ADA).

According to the EEOC, harassment is unwelcome conduct that is based on race, color, religion, sex (including pregnancy), national origin, age (40 or older), disability, or genetic information. Harassment becomes unlawful in either of two situations—when enduring the offensive conduct becomes a condition of continued employment, or when the conduct is severe or pervasive enough to create a work environment that a reasonable person would consider intimidating, hostile, or abusive. Petty slights, annoyances, and isolated incidents (unless extremely serious) usually do not rise to the level of illegality.

Anti-discrimination laws also prohibit harassment against individuals in retaliation for filing a discrimination charge, testifying, or participating in any way in an investigation, proceeding, or lawsuit under these laws. Similarly, harassment in retaliation against somebody who is opposing employment practices that they reasonably believe discriminate against individuals and violate these laws, is also prohibited.

What constitutes offensive conduct? It often includes, but is not limited to, offensive jokes, slurs, epithets or name calling, physical assaults or threats, intimidation, ridicule or mockery, insults or put-downs, offensive objects or pictures, and interference with work performance.

Harassment can occur in a variety of circumstances and settings. The harasser may directly supervise the victim, or he or she may work in a different area of the enterprise. The harasser may also be a vendor, contractor, or agent of the employer. The victim may be a workplace invitee who is not employed with the company. And the victim does not have to be the person harassed; he or she can be anyone affected by the offensive conduct. Finally, it is important to remember that unlawful harassment may occur without economic injury to, or discharge of, the victim.

**Sexual harassment.** Harassment sometimes escalates to sexual harassment, which includes unwelcome sexual advances, requests for sexual favors, and other types of verbal or physical harassment of a sexual nature.

Sexual harassment is defined as either quid pro quo or hostile environment.
ASIS EUROPE 2018
FROM RISK TO RESILIENCE
ROTTERDAM NETHERLANDS 18–20 APRIL 2018

OPENING KEYNOTE BY:
TOM RAFTERY
Global VP, Futurist, Internet of Things Evangelist, SAP

MORE INFO ON WWW.ASISEUROPE.ORG
DO NOT DISCOUNT ANY REPORTS OF HARASSMENT. OFTEN VICTIMS WILL HINT ABOUT LESS OFFENSIVE CONDUCT TO TEST THE WATERS.

According to the EEOC guidelines, quid pro quo harassment occurs when an individual's rejection of or submission to unwanted conduct is used as the basis for employment decisions affecting that individual. Hostile environment harassment occurs when submission to unwelcome sexual conduct is made (either explicitly or implicitly) a term or condition of an individual's employment.

However, the line is often unclear regarding quid pro quo and hostile environment harassment claims. For example, hostile environment harassment may acquire characteristics of quid pro quo harassment if the offending supervisor abuses his or her authority over employment decisions to force the victim to endure or participate in unwanted sexual conduct.

Sexual harassment may culminate in a retaliatory discharge if the victim tells the harasser or employer that he or she will no longer submit to harassment, and is then fired in retaliation for this protest. Under these circumstances, it is appropriate to conclude that both harassment and retaliation in violation of U.S. federal law have occurred, according to the EEOC.

**Sexual assaults.** Sexual harassment can sometimes turn into a sex crime. These crimes can range from rape and battery to other criminal offenses, and they call for law enforcement investigation and potential criminal prosecution. Too often, employers and their investigative teams fail to recognize that the victim is reporting a crime, not just work-related harassment.

**Abuse patterns**

Sexual harassers and offenders frequently demonstrate certain patterns of misconduct. Perpetrators often leverage their power and control over the victims, especially if the victim is an employee. In fact, some offenders carefully seek victims they believe to be vulnerable, who have too much to lose to report inappropriate behavior.

In these cases, the perpetrator may use intimidation tactics to demonstrate control over the victim’s position with the enterprise. Moreover, he or she may engage in emotional abuse, especially if the victim feels trapped because he or she needs the job.

A major warning sign is an attempt to isolate the victim. This may start when the one with the power communicates a desire to mentor and help the intended target. Then, the mentoring may progress so that moments of emotional intimacy are created. This can make the victims feel as if they voluntarily put themselves in the situation by sharing personal experiences. Moreover, if the victim shares some intimate secrets in these conversations, the perpetrator may later use them for emotional blackmail, to secure the victim’s silence.

Sometimes, the victim discusses personal relationships, which may lead to sexual revelations. Once the hook is set, the harasser can make the victim feel complicit in an inappropriate workplace emotional or physical affair, but that does not minimize the seriousness of the harasser’s behavior.

If confronted, offenders often take pains to minimize questionable conduct. They may say they were only joking or blame the victim (or others) for the offensive behavior. They will usually deny any wrongdoing during initial interviews, because they know it is their word versus the word of a powerless victim. They may posture their power to further intimidate the victim: “I’ve been with the company for years and am well-respected. No one will believe you!”

And in some cases, offenders will use their position of authority and apply economic pressure. Executives often have the power to promote, demote, or sabotage a subordinate’s career path. For abusers, these can be powerful tools of oppression to wield, because victims often feel that no one will believe them, and they cannot afford to lose earning power.

**Conducting investigations**

Creating and conducting a neutral and fair investigation is critical to the successful resolution of harassment complaints, but employers must be careful.

As a framework, it is important for organizations to establish investigation-related policies, procedures, and an enterprise-wide training program, and to maintain a culture that encourages victims to report misconduct.

Most enterprises in these situations turn to outside experts, especially when working with legal counsel. Here, experience is crucial; skilled investigators who have years of experience conducting sensitive investigations of sexual misconduct are valuable assets. Too often, inexperienced investigators leave the employer with no evidence and a “he said, she said” inconclusive finding. By keeping some important investigative steps in mind, security professionals can maximize the likelihood of reaching a conclusive investigative result.

First, do not discount any reports of harassment or misconduct. Often victims will hint about less offensive conduct to “test the waters.” In these cases, the victim may want to know that you care and will believe him or her before they disclose the full seriousness of the conduct.

Of course, this does not mean everyone reporting misconduct is telling the truth, or the whole truth. In some instances, accusers may use claims as a preemptive measure to avoid being disciplined or discharged, because they have been forewarned that their
**Questioning THE ACCUSED**

Here are some examples of open-ended questions, along with warning flags that can lead an investigator into a more useful inquiry:

<table>
<thead>
<tr>
<th>What does Mary know about you personally?</th>
<th>How many times have you met with Mary alone in the past six months?</th>
<th>What did Mary share with you about her life?</th>
<th>Who should we interview about Mary and what will they say?</th>
<th>Assume we believe Mary, what do you think should happen?</th>
<th>When we interview past and present employees, how many will say that you talked about private or sexual matters?</th>
<th>What do you believe Mary has said about you?</th>
</tr>
</thead>
<tbody>
<tr>
<td>The accused shares intimate details that superiors have little reason to know about their employees.</td>
<td>The accused makes excuses for meeting with the employee alone.</td>
<td>The accused shares intimate details that superiors have little reason to know about their employees.</td>
<td>The accused attacks Mary by listing all the reasons she cannot be believed, while being unable to name potential witnesses. He or she may name trusted colleagues who can comment only about his or her performance and who have little information about Mary.</td>
<td>Often, a perpetrator seeks mercy or a second chance.</td>
<td>Instead of an immediate and clear denial, the accused will have difficulty remembering.</td>
<td>The accused reveals personal or intimate information.</td>
</tr>
<tr>
<td>The accused blames the employee for wanting to meet alone.</td>
<td>The accused blames the employee for wanting to meet alone.</td>
<td>The accused claims to have a bad memory and can’t recall how many times he or she has met with the employee alone, much less the context and content of such meetings.</td>
<td>The accused attempts to throw other employees under the proverbial bus, although no problems were previously reported.</td>
<td>The accused personalizes the outcome to minimize the chances of being dismissed or publicly ridiculed.</td>
<td>The accused does not believe the supervisor should be harshly punished.</td>
<td>The response of the accused mirrors the statement that the accuser provided about the misconduct.</td>
</tr>
</tbody>
</table>

**Why should we not believe Mary?**

- The accused may come in armed with reasons she cannot be believed, even though previous evaluations about Mary have been stellar.
- The accused may use rank, length of service, and position as reasons to believe him or her, instead of answering the question directly.
- The accused may attack Mary by listing all the reasons she cannot be believed, while being unable to name potential witnesses. He or she may name trusted colleagues who can comment only about his or her performance and who have little information about Mary.
- The accused may come in armed with reasons she cannot be believed, even though previous evaluations about Mary have been stellar.
- The accused may use rank, length of service, and position as reasons to believe him or her, instead of answering the question directly.
- The accused may come in armed with reasons she cannot be believed, even though previous evaluations about Mary have been stellar.
- The accused may use rank, length of service, and position as reasons to believe him or her, instead of answering the question directly.
performance or conduct has not met expectations. In these situations, the supervisor should be accompanied by an HR representative or other neutral supervisor in disciplinary meetings.

Similarly, a witness should be present when the accuser is interviewed. To help understand the accuser’s version of events, security managers should ask questions that help clarify encounters, but should avoid leading questions. Never blame the victim for failing to report the matter earlier.

Sometimes, counsel may request that the interviews be video recorded with the consent of those being interviewed. Video recording interviews is a good way to memorialize important statements, but you must be prepared to meet resistance to this request. In case of such resistance, you may explain that video recording is standard procedure, and that it avoids misunderstandings about what was said and helps properly document any remedial actions required by law.

Often, the victim begins the conversation with the statement, “Can I confide in you about a problem?” However, security managers can never commit to secrecy, because they may be compelled to report what they are told. So, the answer must be on point, such as, “Mary, you clearly came to me because you know I care. Tell me what’s on your mind and I’ll tell you what the next steps are that I can take.”

In interviewing the victim, one of the most critical questions that is often overlooked is, “Whom have you confided in about this matter?” More often than not, victims of sexual misconduct share with trusted confidants. So, ask victims what they revealed, and when they shared the information. This will provide important witnesses who can help corroborate the victim’s integrity. Be careful about immediately believing reports of misconduct that occurred years ago without corroborative testimony or evidence. It does not mean the accuser is being untruthful, but time diminishes evidence and memories.

INTERVIEWING THE ACCUSED

Interviewing the accused is another important step. Too often the accused is interviewed too early in the investigation; before all circumstances are known. Another common misstep is asking closed-ended questions that can make it easier to deny the allegations, such as, “Did you touch Mary in your office last week?”

Questions that are open-ended but targeted are critical to helping determine the truth, and developing them in advance can help determine a successful outcome. (See page 41.)

During the process, it is imperative that the accused and accuser be separated to avoid claims of retaliation. Communicate clearly to the accused that he or she is not to speak to the accuser, or engage in any behavior that may be interpreted as unlawful retaliation. If the accuser is a direct report of the accused, the latter should be transferred. Transferring the accuser to another manager, absent written consent by the victim to be reassigned, can result in a claim of retaliation.

Preserving evidence is vital to the investigation. Emails, text messages, voice mails, work schedules, diaries, and other evidence must be properly documented and preserved. Practicing this consistently is often the key to uncovering evidence that proves or disproves the allegations.

Finally, remember that documentation is the investigator’s salvation. Every step, every interview, and every finding should be clearly documented. The investigation must be fair and neutral to all parties. Decisionmakers will draw conclusions based on the investigative findings; the investigator’s role is to assemble the facts, so they can fully inform the conclusions.

EMPLOYER LIABILITY

The employer is automatically liable for harassment by a supervisor that results in a negative employment action such as termination, failure to promote or hire, or loss of wages. If the supervisor’s harassment results in a hostile work environment, the employer can avoid liability only if it can prove that it reasonably tried to prevent and promptly correct the harassing behavior, and that the employee unreasonably failed to take advantage of any preventive or corrective opportunities provided by the employer.

The employer will be liable for harassment by nonsupervisory employees or nonemployees over whom it has control (for example, independent contractors or customers on the premises) if it knew, or should have known, about the harassment and failed to take prompt and appropriate corrective action.

When investigating allegations of harassment, the EEOC looks at the entire record, including the nature of the conduct and the context in which the alleged incidents occurred. A determination of whether harassment is severe or pervasive enough to be illegal is made on a case-by-case basis.

PREVENTION IS KEY

Prevention is the best tool to mitigate harassment in the workplace. Establish clear anti-harassment policies and
procedures, provide training at all levels, and take immediate and appropriate action when an employee complains. Clearly communicate to employees that unwelcome harassing and sexual misconduct will not be tolerated. In addition, employees should be encouraged to both inform the harasser directly that the conduct is unwelcome and must stop, and report harassment to management at an early stage to prevent its escalation.

Employers should strive to create an environment and a work culture in which employees feel free to raise concerns and are confident that those concerns will be addressed. The result will be a positive workplace where all personnel are valued.

A RUSH TO JUDGMENT

As seen in recent events, employers are often quick to distance themselves from the accused prior to any investigation. This response hurts the enterprise and brand, because it sends a message of a rush to judgment, or damage control. The first public response, if any, is to communicate that the company takes all allegations seriously, conducts a thorough investigation, and then takes effective remedial steps.

The EEOC does not demand termination, but it does require that companies take effective remedial steps. Termination may be warranted, but the investigation will determine the ultimate disciplinary measures. Ask the accuser what he or she thinks should happen to the perpetrator. Listening to this proposed solution often mitigates the risk of civil claims, because the accuser was part of the investigation, apprised of the findings, and involved in determining the appropriate remedial steps.

If your organization has not equipped itself to perform a thorough and fair investigation, it may decide instead on a hasty termination, or an immediate distancing from the accused. This is a mistake. If made, the next time you get to hear a response from the accused may be in a deposition in a costly and highly public civil lawsuit. Or worse, in a criminal court.

STEVEN C. MILLWEE, CPP, IS THE FOUNDER, PRESIDENT, AND CEO OF SECURTEST, INC., A BACKGROUND SCREENING AND INVESTIGATIVE CONSULTING FIRM. MILLWEE WAS THE 2002 PRESIDENT OF ASIS INTERNATIONAL. HE IS A FREQUENT EXPERT WITNESS IN SEXUAL HARASSMENT CASES, AND IS THE AUTHOR OF SEVERAL HARASSMENT AND SEXUAL ASSAULT BIOGRAPHICAL QUESTIONNAIRES FOR USE IN INVESTIGATIONS.
U.S. gun laws vary by state, and employers must carefully consider the legal landscape when crafting policies and procedures.

In late 2017, a photograph surfaced of three construction workers from American Sewer Services carrying weapons on a job site in Milwaukee. In the photo, two men clearly displayed their weapons in holsters, while another held a pistol in his hand.

As a result, the three construction workers were fired. The city of Milwaukee cited its policy that prohibits employees from bringing weapons to their jobs, including employees of subcontractors.

One gun advocate defended the workers and said the geographic area where they carried their weapons was “infamous” for its crime rate, *The Blaze* reported.
On the other end of the spectrum, a Wisconsin state legislator told the media outlet that carrying guns openly on the job was “irresponsible.”

While the city of Milwaukee has a clear policy on guns, for most private employers, the issue is anything but cut-and-dried. There is currently no U.S. federal law regulating weapons at private workplaces, but many state legislatures have taken up the cause of protecting the Second Amendment rights of employees while on the job. These laws, which are typically designed to protect employees’ individual rights to possess concealed firearms, vary in terms of their restrictions and make it tough for employers operating in multiple U.S. states to implement one weapons policy across the board.

Workplace shootings have become increasingly common in the United States over the last few decades. The number of these incidents rose 15 percent in 2015 to 354 shootings, according to the latest numbers from the U.S. Bureau of Labor Statistics, and resulting homicides grew by 2 percent that year.

Gun advocates cite such cases as reasons to allow guns in the workplace, while critics say these shootings are exactly why employers should ban firearms. As the debate rages on, employers are left grappling with the question of how to comply with state law and institute their own policies that promote a safe work environment. While there are many legal twists and turns surrounding the issue, security practitioners must deal with the question of how current laws affect their responsibility to keep employees and property safe from external and internal threats.

By understanding the legal landscape surrounding firearms on work property, and ensuring that existing policies and procedures properly address workplace violence, security professionals can help promote a safe work environment without infringing on the legal rights of their employees.

**Parking Lot Laws**

Most commonly, workplace gun laws allow employees the right to have firearms in their locked, private vehicles while parked on company-owned property. Additional obligations may be placed on the employer, such as a prohibition on searching vehicles and discriminating against an employee because he or she is a gun owner.

Twenty-three U.S. states provide some level of protection for employees who bring their firearms to company property. These so-called “parking lot laws” were part of an effort by state legislatures in the early 2000s to allow workers...
to exercise their Second Amendment rights at work, with some restrictions.

For example, often the gun must be locked in the trunk or glove box, or be hidden from view through the vehicle’s windows. But the business community sees many issues with these laws and fears they will have a far-reaching impact on both employee safety and legal liability.

Parking lot laws vary in the level of protection they offer gun owners. Most prohibit employers from asking workers if they own guns, and from firing employees for owning firearms. These laws frequently conflict with existing workplace policies, which limit the employee’s ability to bring firearms to work.

Oklahoma was the first U.S. state to pass a parking lot law when it amended legislation in 2004 to protect firearm owners from weapons prohibitions in workplace parking lots.

In 2002, an Oklahoma employer terminated several employees for having guns in their vehicles, which were parked on the employer’s property. In response to the outcry that followed, the Oklahoma legislature amended the Oklahoma Self-Defense Act to ban employers from establishing any policy or rule that has the effect of prohibiting employees from transporting and storing firearms in a locked vehicle that is parked in employers’ lots.

This caused great concern among the business community, which felt certain that the law would not survive legal scrutiny. In response, a group of Oklahoma employers challenged the state law, arguing that the legislation conflicted with the U.S. Occupational Safety and Health Administration (OSHA) general duty clause, also known as the Occupational Safety and Health Act of 1970 (OSH Act), a U.S. federal law.

The plaintiffs argued that the general duty clause says employers must maintain a safe and secure workplace free of violence, and preempts any existing U.S. state law. The U.S. District Court for the Northern District of Oklahoma agreed with the employers.

The district court reasoned that under the general duty clause, gun-related workplace violence is a “recognized hazard.” Therefore, any employer allowing firearms in the workplace lot may be in violation of U.S. federal law by promoting an unsafe workplace.

The case went to the U.S. Court of Appeals for the Tenth Circuit, which reversed the decision. The court reasoned that “OSHA has not indicated in any way that employers should prohibit firearms from company parking lots,” according to court documents. “OSHA’s website, guidelines, and citation history do not speak at all to any such prohibition.”

Because OSHA does not indicate that employers should prohibit firearms from company parking lots, the appellate court ruled that there is no U.S. federal law that would preempt Oklahoma’s amendment to the Self-Defense Act.

This initial case was a signal that employers would not be able to simply dismiss these laws by citing safety and security concerns or by arguing that U.S. federal regulations created an obligation to keep the workplace free of employees’ weapons.

**Employee Rights**

More lawsuits can be expected regarding employee termination based on gun-free workplace policies. An intriguing case comes out of the state of Florida, which passed a comprehensive law in 2008 that prohibits public and private employers from discriminating against any employee, customer, or invitee for exercising the right to keep and bear arms.

Under the Florida law, employers are barred from many actions, including: prohibiting employees or invitees from possessing legally owned firearms in their vehicles; inquiring about the presence of a firearm in the employee or invitee’s vehicles; searching a private motor vehicle; and taking any action against an employee or invitee based on any verbal or written statement regarding the possession of a firearm in a private vehicle.

The law also says that companies are barred from conditioning employment on the following: whether an employee or prospective employee holds a concealed-weapons permit; an agreement by the employee or prospective employee that forbids the employee from keeping a legal firearm locked in his or her vehicle when the firearm is kept for lawful purposes; or prohibiting any employee or invitee from entering the parking lot because the employee or invitee’s vehicle contains a legal firearm.

Finally, the law bars employers from terminating or otherwise discriminating against an employee or expelling an invitee for exercising the right to keep and bear arms or to exercise self-defense, so long as the firearm is not exhibited on company property for any reason other
More lawsuits can be expected regarding employee termination based on gun-free workplace policies.

than lawful defensive purposes.

In December 2015, an employee who worked for Universal theme park in Orlando, Florida, had a concealed weapon in his vehicle in the employee parking garage. The employee, who had worked for Universal since 1993, commonly left his gun in his car at work. One day, the handgun was stolen from his vehicle, and he reported it to the police.

When park officials learned that he had a firearm on company property, they terminated him, claiming that he had violated Universal’s gun-free zone policy.

The employee sued Universal in Orange County Circuit Court, citing the 2008 law. The lawsuit argued that he had an express right to bring his gun onto the lot and leave it in his vehicle.

Universal claimed that the Florida law didn’t apply because schools and prisons are exempt from state weapons policies, and Universal has a program for school children on its property. Before the litigation could play out, Universal gave the employee his job back in April 2016 and he withdrew the lawsuit, the Orlando Sentinel reported.

Comparable cases have been filed in similar circumstances in other states. In Kentucky, a man was fired from UPS Supply Chain Solutions in May 2013 for transferring a gun lawfully stored in his personal vehicle to another worker’s personal vehicle.

The man, who had a concealed carry permit, said he experienced car trouble on the way to work, and moved the weapon because he was taking his car to be repaired. The fellow employee storing his weapon as a favor soon became uncomfortable and reported it to his supervisor.

The company then placed the employee on suspension and eventually fired him, citing that its policy only allowed for weapons inside a private vehicle. The company claimed that by removing the gun from his personal vehicle, he violated the workplace policy.

In the lawsuit, the employee claimed that under a Kentucky Revised Statute, a firearm may be “removed from the vehicle or handled” when it is done so in “defense of property.”

But the court ruled that the employee was attempting to interpret their law too broadly. “However inclined we might be to believe that such an exception would be a good thing, we decline to construe the term ‘defense of property’ as broadly as the employee suggests,” the court wrote. (Holly v. UPS Supply Chain Solutions, Inc., U.S. Court of Appeals for the Sixth Circuit, March 2017)

Employer Protections

Several U.S. states have included some liability protections to provide conditional immunity to employers that comply with their state’s guns-at-work law. This is mainly in response to the business community’s outcry over what liability they will face for workplace violence involving guns on their property.

For example, under Georgia law, an employer is not liable for any criminal or civil action for damages arising from an occurrence involving the transportation, storage, possession, or use of a firearm, including theft of the firearm, unless the employer commits a criminal act involving a firearm, or if the employer knew the person using the firearm would commit a criminal act on the employer’s premises.

While the Georgia law provides some cover for employers, it also leaves them vulnerable to lawsuits if they knew the person would commit an act of violence. This raises many questions as to how to handle someone who may have violent tendencies. How do you restrict that person’s access to firearms in his or her vehicle? Can you terminate him or her based on that assumption alone?

Policies. Although these laws at face value complicate certain aspects of workplace violence policies and active shooter response plans, there are many steps that employers can take. Most importantly, security practitioners should educate themselves on relevant U.S. state guidelines, and confer with their general counsel on these issues to avoid unknowingly breaking the law.

For example, signs that read “no weapons” in parking lots are illegal in some U.S. states in certain circumstances. Knowing the limitations will allow companies to properly respond without risking legal liability.

If located in a state with current legal provisions for weapons in the workplace, companies should educate their workers on the boundaries of that law. For example, some employees will unintentionally assume they have greater rights, such as open-carry or storing the weapon inside the workplace.

Workplace violence. Policies on workplace violence should include a thorough explanation of relevant state law regarding guns on workplace property. Employers should be comprehensive in creating policies that outline how to report and respond to employees who are potentially violent or otherwise pose a threat to the safety of others.
Many employers lose their conditional immunity in a workplace shooting or incident if the perpetrator was someone who had a history of violence, or was otherwise known to the employer to be a threat.

In U.S. states that make provisions for weapons on workplace property, conducting high-risk terminations are of greater concern. Employees who store weapons in their cars, abiding by the law, could inadvertently become a threat during termination.

When firing any individual considered to be high-risk, companies should consider providing a security escort to the parking lot. Security should ensure that the former employee has left the property, and front desk or other reception team members should be alerted that the person is not allowed back on the premises. Organizations should train security officers, as well as human resource employees, in the use of de-escalation techniques.

Finally, for workplaces that must comply with parking lot laws, there are several steps that will help protect the employer while respecting the legal rights of employees. Organizations may consider increasing security in parking areas, such as adding an access control point; conducting patrols around the building and in parking lots; installing or enhancing video surveillance systems; and implementing proper lighting.

In some cases, bag searches or magnetometers may be installed at building entry points, but legal requirements should be checked before implementing such measures. Deterring the carriage of weapons outside the vehicle will generally serve as a reminder of the law and keep both employers and employees safe.

At first glance, the laws surrounding weapons in the workplace may seem like a jigsaw puzzle that is difficult to comprehend, but there are steps employers can take to ensure that assets and people are protected. Understanding the law and establishing strong policies within the employers’ legal rights will ensure that workplaces abide by the law while keeping their assets and people safe.

Eddie Sorrells, CPP, PCI, PSP, is Chief Operating Officer and General Counsel at DSI Security Services in Dothan, Alabama. He is the author of Security Litigation: Best Practices for Managing and Preventing Security-Related Lawsuits. He can be reached at esorrells@dsisecurity.com.
The latest *State of the American Workplace* report, the Gallup company’s look at management practices in the U.S. workplace, contains some grim news. A clear majority of employees are not engaged with their jobs, and employers are finding it increasingly hard to retain quality workers. “The very practice of management no longer works,” Gallup Chairman and CEO Jim Clifton says in the report, which was published last year.

But the experts at Gallup also argue that employee engagement and retention can be markedly improved—through effective coaching. Managers who are effective coaches often possess certain abilities and attributes: they are usually clear and insightful explainers; they have an aptitude for building on an employee’s strengths; they are adept at working with different learning styles; and they can maintain patience in the face of mistakes.

But effective coaching is a two-way process. And just as talented coaches share certain traits, employees who are highly coachable often possess a cluster of certain qualities and abilities. These attributes can be thought of as “green flags”—indicators that the employee is driven and prepared to grow and improve on their existing skill sets, to learn new skills, and to “correct performance without resentment,” in the words of legendary UCLA basketball coach John Wooden.

In the security field, these green flags can include demonstrated honesty, adaptability to change, intellectual curiosity and love of learning, interpersonal skills, attention to detail, problem-solving abilities, resourceful thinking, safety awareness, a reasonable level of suspiciousness, and emotional intelligence.

Smart security managers have realized that these green flags often serve as predictors of future success, and so they have focused on fine tuning this list of qualities and attributes. It has value in the screening and hiring process, as well as in managing employees once they are hired, especially in organizations that are going through performance changes or improvements.

And being coachable is not just important for front-line security workers. Managers, too, need to remain coachable, so that they can continue to improve and grow, and ultimately become better coaches.

The following examples are taken from real-world situations in the security industry—the names of the managers have been changed—and illustrate these concepts. They provide best practice in the ever-evolving security industry, employees who respond well to coaching are invaluable. Here’s how to assess coachability and ensure that both workers and managers remain open to continuous improvement.
guidance for security leaders on what to look for in terms of an employee’s coachable potential, and how managers can also benefit from becoming more coachable themselves.

**Success via Coachability**

John Smith worked in the criminal justice public sector for a little over 20 years in the Midwest. Under his leadership, his department achieved and maintained accreditation, with high scores on all metrics. Turnover in John’s department was low; he had helped build a positive team atmosphere with high levels of employee engagement and job satisfaction.

Still, John silently complained to himself about being overworked and underpaid. One day, he saw a security director position advertised by a privately owned security company in the Omaha area. He decided it was time for him to put up or shut up, and see if he could get paid his real worth. So, John moved forward on this new opportunity, and in so doing stumbled upon the importance of coachability.

As it happened, the owner of the security company in question also ran the largest maid service franchise in the world and was a graduate of Harvard Business School. John was applying for the position of general manager; the previous general manager was a retired FBI agent who at first dazzled the owner with his training and work history, but soon showed that he lacked the main ingredient the owner needed to grow the security company—coachability. And so, it wasn’t long before both decided to end the relationship.

Conversely, John possessed a few green flags of coachability the owner wanted to see in the applicant for his open general manager position—adaptability, intellectual curiosity, and a penchant for further learning and improvement.

During the interview and candidate evaluation process, these qualities became evident to the owner. For example, John discussed how he had adjusted to living in a foreign country during his public-sector career. Before that, he had successfully changed careers from mental health to corrections. He had completed his master’s degree, which reflected an interest in further learning. He demonstrated that he was interested in moving from a safe, structured public service job to the greater unknowns of the private sector, where he would have to think on his feet and create the structure that worked best for the company. Throughout the interview, John asked insightful questions that showed strong intellectual curiosity.

These attributes made the owner feel he was hiring what he needed most—a security manager whom he could mentor so that the manager would develop his own coaching skills to build the right workforce.

John got the job, and went on to a second career in the private sector, where he thrived for another 20 years. He was especially successful in recruiting and hiring an impressive team to grow the business. In hiring, he didn’t look for clones of himself in terms of education, skill sets, and temperament. Rather, the common denominator he did look for was an insatiable drive to learn, grow, and improve, which was usually accompanied by high engagement with and passion for the work.

**Coachability for Managers**

As a security manager for a medium-sized corporation on the East Coast, Mary Jones learned the importance of coachability and how it complemented the two-way management style she had learned in earlier training.

She decided to take on her company’s two-pronged problem of hiring and retention; she set her sights on reducing the failures of bad hiring and the costs of high turnover. Mary realized that identifying the green flags of highly coachable applicants went a long way toward making better hires, and she became proficient in determining this by asking probing questions during the interview process.

One such question was: “When you start a new job, do you prefer to look for opportunities to apply what you already know from past experience, or do you try to learn something new about what you don’t know? Tell me about how you learned about which way to approach a

**In hiring, he didn’t look for clones of himself in terms of education, skill sets, and temperament.**
and practice how this style of interviewing would get better results. Mary’s efforts did not stop there.

Once hiring had improved, Mary also wanted to improve the retention rate of coachable employees. Thus, she developed a custom-designed training program by gathering new ideas from a variety of resources and programs from professional HR organizations that were available online for free, and then carefully updating ideas from few of her own coaching and counseling training programs.

She then provided summary information about this new training to all her supervisors, aimed at rekindling their own coachability, which would help the supervisors learn how to better identify coachable employees at the same time. The training was well-received and everyone was motivated towards a common goal.

Under Mary’s efforts, managers learned how to hire employees with excellent coachability potential by asking better questions and spotting tell-tale answers. Supervisors learned how to improve their coaching abilities by practicing new mediation strategies. And employees were able to improve upon the coachability potential they first brought to the job. This was a win-win-win for Mary, her supervisors, and the company at large.

Assessing Coachability
During Bob Miller’s long career in security management, his understanding of the importance of coachability evolved, and an examination of this evolution reveals some guidance for managers assessing coachability.

Early on, Bob discovered that there was an X-factor in an employee’s ultimate success that was just as important as the knowledge, skills, and abilities that are asked for on the application for federal jobs. Bob’s discovery was in part due to his own self-awareness—he was aware of his own insatiable drive to become better at whatever he was doing, and this helped him spot the same drive in the applicants he screened and interviewed.

Given his belief in the great value of coachability, he revised the hiring process he had traditionally used. He discarded practices he now considered time-wasters, such as checking references about the candidate’s honesty and dependability, verifying prior work history and education, and administering psychological testing. Using the Occam’s razor principle, he ended up with the one prevailing trait that he found was most predictive of success (after the applicant’s résumés proved baseline professional competency)—an openness to learning, growing, and improving.

From here, Bob designed a behavioral interview with a set of telling questions designed to get revealing answers regarding a person’s drive to succeed as a security officer or supervisor. In most cases, this drive starts with the candidate’s acceptance that they do not know it all already, so the interview questions were also designed to gauge if that acceptance had been established. Given the unknowns and new developments of security work today, this type of acceptance is critical to future success.

Bob constructed his list of probative interview questions so that it would be difficult for applicants to hide behind hypothetical or general, unrevealing answers. He first posed a set of written questions, so the candidate could take some time to think and draw on their most relevant past experiences. Then during the interview, Bob and the candidate could discuss these preliminary answers in more detail, so that the applicant’s coachability could be assessed.

In terms of specifics, the written list of questions started out asking applicants about past failures and how they overcame them. Then, during discussion, candidates were asked for examples of how they had used common sense to get results in previous situations, areas in which they felt they could improve, what they liked and disliked about their best supervisor, and what they thought an employee had to demonstrate to be successful in security work. Further discussion of the answers to these five simple questions proved to be revealing, and an effective means to assessing coachability potential in the applicants.

The good answers included ones with enough detail to face-validate their actual occurrence, such as “I liked my previous supervisor’s patience with me when I didn’t succeed at a task delegated to me. She gave me some useful feedback and immediate suggestions to improve the next time. What I didn’t like about her was that she was always busy and difficult to get time with. However, I guess I should have mentioned this problem to her.”

The bad answers lacked such detail, or even sidestepped the question, such as, “I didn’t really get to know my supervisor that well,” or “I’d rather not get into that.” Of course when the applicant couldn’t stop listing all the previous supervisor’s faults and was not able to come up with any good things to say about the supervisor, that was a big red flag of cynicism in his coachability.

The process worked well, but Bob, being of a continuous improvement mindset, knew he wasn’t finished in his efforts to perfect his assessment method for determining what level of coachability each applicant was bringing to the job. Interviewing is like standardized testing; eventually, the best answers to even the most highly guarded LSAT questions become common knowledge. Bob anticipated this would eventually happen with his coachability assessment questions, so he continued to revise them to stay ahead of the curve. For example, one question that consistently showed value was, “Tell me about the best sports or activities coach you had in school, and what do you think made him so successful?” He revised this by expanding it, and it yielded even greater value: “What characteristics of this coach have you applied in your own life?”
Removing Obstacles
Can a security employee be taught to be coachable? Security manager Michelle Palmer wanted to explore this possibility with her direct reports. Many members of her staff did not seem to see the value in coachability, or why it was necessary. Fortunately, Michelle knew the importance of explaining concepts well enough to sell them, thus removing the resistance.

She realized that one of the main roadblocks for her employees was their natural defensiveness in receiving feedback about themselves. She decided to use personal examples to make her explanations more effective. For example, she shared how she personally overcame her own obstacles in becoming more coachable, including her original unwillingness to share her own vulnerabilities, to become more open to different perspectives other than her own, and to accept the risk that came with experimenting with new behaviors.

In her managing, Michelle also employed another lesson she learned previously in becoming more coachable. She replaced her usual relaxed approach in some staff interactions with a more assertive posture. For example, in giving feedback to others, she often replaced “you,” such as in “it would be good if you did this differently,” with “I,” such as in “I would like you to try doing this in such-and-such way.” This shift had a positive effect; staff members became much less defensive, and better listeners.

Finally, Michelle’s instruction was made more effective by a key realization—all she thought she knew to be true about the security profession wasn’t necessarily so. Her own growth had been somewhat stalled by this limiting perspective, and once she was free from it, she could better communicate the value of staying open to new ideas and continuous growth and improvement.

Coaching the Future
If a security manager is successful in hiring coachable employees, and can help existing staff remain coachable, a culture and system of proactive performance improvement can be maintained in the security department. In such a culture, managers and employees continue learning and improving.

WILLIAM COTTRINGER, PHD, CERTIFIED HOMELAND SECURITY (CHS) LEVEL III, IS EXECUTIVE VICE-PRESIDENT FOR EMPLOYEE RELATIONS FOR PUGET SOUND SECURITY PATROL, INC., IN BELLEVUE, WASHINGTON, AND ADJUNCT PROFESSOR IN CRIMINAL JUSTICE AT NORTHWEST UNIVERSITY.
REGISTER TODAY!

Make plans now to join 2,200+ security and law enforcement professionals at ASIS NYC 2018, the Northeast's most anticipated security conference and expo.

This two-day event delivers essential security solutions from 110+ exhibitors, high-level peer networking, and top-notch education sessions examining critical issues and trends in enterprise risk and public safety.

Join us in honoring the 2018 “Person of the Year”

— TIMOTHY CARDINAL DOLAN
Archbishop of New York

asisonline.org/NYC

WIN AN APPLE WATCH!

Be sure to enter promo code NYSM1 when registering for your chance to win. Visit asisonline.org/win for details.
The program included an update on the ASIS Strategic Plan from ASIS International CEO Peter J. O’Neil, CAE, and Senior Manager Adam Savino. O’Neil and Savino touched upon progress made regarding Board directives, which include branding, global network, professional competency, organization and operations performance, knowledge and learning, and enterprise security risk management.

The ASIS Foundation’s Scouting the Future research workshop identified issues that today’s security managers consider most important in the years ahead. Attendees were presented with 15 different change drivers affecting the security industry, and were asked to choose which of these topics they consider most pressing. Their responses will inform ASIS Foundation research over the coming months.

On January 18 the Society held its Annual Business Meeting. ASIS International Chairman of the Board Thomas J. Langer, CPP, began by honoring David C. Davis, CPP, and Darryl Branham, CPP, for their service on the Board of Directors. Next, more volunteer leaders were honored for their extraordinary service to the Society. Bob Oatman, CPP, was named the 2017 Council Chairman of the Year for his leadership of the Executive Protection Council. Marco Meza Sandoval, Region 7C, was named 2017 Regional Vice President of the Year, and Bob Johnson, CPP, Group 5, was named 2017 Senior Regional Vice President of the Year.

Christina Duffey, CPP, presented the treasurer’s report, which provided an overview of the financial health of ASIS, and 2018 President Dick Chase, CPP, PCI, PSP, outlined his priorities for 2018.

Evening events included a Casino Night, which raised more than $5,000 for the ASIS Foundation, and the President’s Reception, which celebrated the start of Chase’s tenure as president.

The conference concluded with a presentation by the FBI and volunteer roundtables. To view event pictures, visit flickr.com/asisinternational.
Together with the new ASIS website launch in late January, the Society introduced a new certification application process that makes it easier for candidates to understand exam requirements and apply for certification. The Professional Certification Board implemented several changes to its policies in support of the new application process.

Newly certified professionals’ three-year certification cycle begins on the day they pass the exam and ends three years later, at the end of that month. Those whose cycles end on December 31 will continue to have their cycles end at the close of the calendar year.

Those who sit for the exam three times during their two-year testing eligibility period without passing it may reapply as soon as their eligibility period expires (but at least 90 days after their third attempt). Previously, candidates had to wait 18 months from the time of the third attempt.

As part of the new user-friendly recertification application process, ASIS staff will no longer verify each continuing professional education credit (CPE) as it is reported. As before, certificants will use the online application to keep track of CPEs as they are earned. When they submit their recertification applications, the CPEs will be reviewed all at once.

The grace period for recertifying after a certification cycle ends has been reduced from one year to three months. Addition-
ally, all CPEs must be completed during the three-year cycle (none during the grace period).

“These changes will make it easier than ever for security professionals to become certified and stay certified,” says ASIS International Certification Director Gayle Rosnick. “These updates will help lay the groundwork to support a larger and broader pool of certificants in the years to come.”

In addition, the Certification Department has received Board approval to begin investigating an early-career certification. In January a dozen early careerists attended a two-day program at ASIS headquarters to determine the relevant competencies for a new early-career security management certification. Work will continue on this initiative throughout 2018.

For more information or to learn how you can pursue ASIS board certification, visit asisonline.org.

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

LIFETIME CERTIFICATION

Congratulations to these individuals who have achieved lifetime certification.

- Krishnamoorthy Arunasalam, CPP
- Paul Stewart Barker, CPP
- Fred A. Buran, CPP
- Dennis G. Byerly, CPP
- Jose E. Campos, CPP
- Salvatore P. DeCarlo, Jr., CPP
- Cheryl D. Elliott, CPP, PCI
- Jeffrey J. Haykin, CPP
- Pearse Healy, CPP
- Eugene Hermanny, CPP
- Dan Jenkins, CPP
- Garrett J. Ochalek, CPP
- Shirley A. Pierini, CPP, PCI
- Robert C. Quigley, CPP
- Craig P. Remsburg, CPP
- Thomas J. Rohr, Sr., CPP
- John R. Ryan, CPP
- Kathleen A. Sowder, CPP
- Scott Wells, CPP
- Ian G. Wing, CPP
- Christopher D. Yokley, CPP

MEMBER BOOK REVIEW


The security landscape is evolving at an enormous speed. Volatility, uncertainty, complexity, and ambiguity are the new normal. So, how do you address security challenges in such an environment? The answer is through...
enterprise security risk management (ESRM), an integrated risk-based approach to managing security risks. It brings together cyber, information, physical security, asset management, and business continuity. ASIS has made ESRM a global strategic priority.

In the Manager’s Guide to Enterprise Security Risk Management, authors Allen and Loyear provide a comprehensive overview of the principles and applications underlying the ESRM philosophy. They set the stage in the first part of the book with an introduction to ESRM and share some important insights on the differences between traditional security and the ESRM approach, illustrating their points with examples.

The second part of the book guides the reader through the implementation of an ESRM program. One excellent chapter promotes design thinking as a conceptual model for ESRM. A design thinking approach can provide a unique platform for innovation and overcoming new security challenges.

Finally, the book provides insights and strategies to ensure the success of the ESRM program. It explains what an executive needs to know about ESRM, and gives readers the tools to succeed.

In sum, this guide accomplishes exactly what it set out to do—provide security leaders and managers with the principles and applications to explore, design, implement, and secure the success of an ESRM program.

Note: The authors of this book recently published a more detailed look at ESRM in Enterprise Security Risk Management: Concepts and Applications, also published by Rothstein.

REVIEWER: Rachid Kerkab has almost two decades of experience in criminology, security strategy, risk, and resilience. He is a member of ASIS.

CERTIFICATION PROFILE
LEON BERESFORD, CPP

Leon Beresford, CPP, took classes by day, and worked as a security guard by night. As he picked up his weekly paycheck, he would imagine himself one day sitting in the manager’s office.

He dedicated himself to this goal. He earned a certificate in security management, and soon after, landed an entry-level security management job. The rest is history.

During 30 years in the security industry, Beresford has held increasingly responsible positions with Simon Property Group and Allied Barton Security Services. For the past 11 years, he has worked for Admiral Security Services, a leading security services provider, where he is senior vice president. In this capacity, he has responsibility for all company divisions across six states, and he also has a role in acquisitions.

Each morning, he drops his daughter off at school and spends the rest of his commute on calls with his seven direct reports. From there, his days run the gamut of client relations, business development, planning sessions, risk management, cultivating partnerships with law enforcement, networking, meetings with ownership and internal stakeholders, and ASIS volunteer leadership.

Beresford earned his Certified Protection Professional® (CPP) certification in support of his security management goals. “I wanted to differentiate myself by achieving the highest accreditation in our industry,” he says. “Certification is like the icing on a delicious carrot cake, it increases my credibility as a security management practitioner.”

Beresford is deeply committed to the professionalism that certification brings. He recently “strongly recommended” that certain positions at Admiral attain board certification within the next 12 months.

Admiral paid for the review classes, study materials, and exam fees when Beresford achieved his certification in 2010. In his current role, he pays it forward in support of his team members by hosting study groups and purchasing review resources that candidates can use as they study for the exam.

To anyone considering whether to pursue certification, Beresford offers three words: “Just do it. I started to prep to take the CPP exam several times in my career. Inevitably, I was promoted, moved, or simply had my workload increased, which caused me to delay taking the exam. There will never be an optimal time. I finally just scheduled and paid for the exam. This challenged me to be purposeful in my preparation, and I took the exam and passed. I was so proud to attend my next annual conference with the CPP designation on my badge.”

One of the most rewarding aspects of Beresford’s ASIS membership has been volunteer service. A former chair of the National Capital chapter, he currently serves on the Security Services Council and is assistant regional vice president for ASIS Region 5A.

“My ASIS membership has given me the opportunity to meet so many great security professionals,” Beresford says. “This community of peers has been invaluable to my career. I have developed lifelong friendships and gained access to information and resources I might not have known about if I was not a member.”

PROFILE BY STEVEN BARNETT, ASIS COMMUNICATIONS COORDINATOR
JUDICIAL DECISIONS

BOTNETS. Three men pleaded guilty to creating and operating two botnets used to target Internet of Things (IoT) devices to conduct distributed denial-of-service (DDoS) attacks.

Paras Jha, 21; Josiah White, 20; and Dalton Norman, 21; pleaded guilty to conspiracy to violate the Computer Fraud and Abuse Act (CFAA) by operating the Mirai Botnet. The three men created the botnet in the summer and fall of 2016 and designed it to target IoT devices.

“The defendants attempted to discover both known and previously undisclosed vulnerabilities that allowed them to surreptitiously attain control over the victim devices for the purpose of forcing the devices to participate in the Mirai Botnet,” according to the U.S. Department of Justice (DOJ).

The botnet, at its peak, was made up of hundreds of thousands of devices that were then used to carry out DDoS attacks.

Jha later posted Mirai’s source code on an online forum, allowing other criminal actors to use it for attacks and marking the end of his, White’s, and Norman’s involvement in the botnet.

WAGES
A California judge dismissed a class action lawsuit filed by female Google employees accusing the tech giant of paying women less than men. Superior Court Judge Mary Wiss explained that the plaintiffs must refile to show that specific women were affected by Google’s pay policies—not all women at the company. She also found that two of the plaintiffs had not demonstrated that they performed work comparable to men who allegedly were paid more. (Ellis v. Google, California Superior Court, San Francisco County, No. CGC-17-561299, 2017)

RELIGIOUS CLAIMS
A U.S. federal inmate may have stuffed animals in his prison cell because they are necessary to practice his religion, a U.S. appeals court said in a summary order. Inmate Christopher Grief claimed that he’d owned stuffed animals throughout his life and received spiritual guidance from them during meditation, according to court documents. However, Grief was denied the ability to have them while in custody. He filed suit alleging violation of the Religious Freedom Restoration Act, and an appellate court ruled in his favor after a lower court dismissed the suit. “...we conclude that the district court erred in deciding that Grief’s belief regarding stuffed animals could not plausibly constitute a religious belief,” the appellate court wrote in a summary order. (Grief v. Quay, U.S. Court of Appeals for the Second Circuit, No. 16-1651, 2017)

FRAUD
Former Volkswagen executive Oliver Schmidt was sentenced to the maximum prison term of seven years and fined $400,000 for his role in the car manufacturer’s emissions scandal. Schmidt, who oversaw U.S. emissions testing for Volkswagen, pleaded guilty, and asked for a reduced sentence, which the court did not grant. “You are a key conspirator responsible for the cover-up in the United States of a massive fraud perpetrated on the American consumer,” U.S. Judge Sean Cox said when handing down the sentence, according to The New York Times. (U.S. v. Volkswagen, U.S. District Court for the Eastern District of Michigan, No. 2:16-cr-20398-SFC-APP, 2017)
Following the Mirai project, Jha and Norman went on to create a new botnet that ultimately infected more than 100,000 U.S.-based devices with malicious software. The botnet was then used for advertising fraud.

Jha also pleaded guilty to violating the Computer Fraud and Abuse Act for executing a series of attacks against Rutgers University’s networks.

“Jha’s attacks effectively shut down Rutgers University’s central authentication server, which maintained, among other things, the gateway portal through which staff, faculty, and students delivered assignments and assessments,” the DOJ said. “At times, Jha succeeded in taking the portal offline for multi-day periods, harming Rutgers University, its faculty, and its students.”

Jha, White, and Norman had not been sentenced as of Security Management’s press time, but could face up to five years in U.S. federal prison and a fine of $250,000 for each count of violating the CFAA.

**FITNESS FOR DUTY.** A U.S. federal appellate court granted summary judgment to an employer, finding that a reasonable jury would have found its mental-health examinations of an administrator at a traffic safety office “job related and consistent with business necessity.”

Deanna Painter was assigned to the position of office administrator at Traffic Safety, a division of the Illinois Department of Transportation (IDOT), in September 2010. In the spring of 2011, Director of Traffic Safety Mike Stout became aware of an incident between Painter and a colleague, where Painter accused the person of prank calling her at the office.

Other employees also said that Painter had accused them of spying on her while at work, and Painter admitted that she’d had “issues with several employees,” according to court documents.

Stout wrote to IDOT’s manager of the employee assistance program, explaining safety concerns he had with Painter. He also placed Painter on administrative leave in April 2011, and more employees continued to come forward to disclose issues with Painter and concerns about working with her.

Dr. David Fletcher conducted a fit-for-duty examination of Painter and determined that she was fit for duty. However, he recommended a reevaluation in 45 days for continued observation, based on her pattern of mood swings and speech during the evaluation. His report did not indicate whether he reviewed any employee statements in making his determination.

After Fletcher’s examination, Stout wrote a memo to IDOT’s manager of employee assistance program detailing his concerns for his employees’ safety if Painter were returned to work at Traffic Safety. For instance, during Painter’s leave, two or three employees requested security escorts to their vehicles at the end of the day due to concerns that Painter might approach them.

Painter was sent back to Fletcher for another fit-for-duty exam in July 2011, during which Fletcher said he “reviewed additional documentation that shows disturbing inter-personal skills,” according to court documents.

Fletcher did not make a fitness for duty recommendation; instead, he referred Painter to Karen Lee, a psychologist. Lee began treating Painter and did not submit a copy of her report to IDOT.

In September 2011, Painter returned to work and in October was transferred to day labor—another division of IDOT—as an office administrator. She then began keeping a daily detailed log of her colleagues’ actions and conversations.

The purpose of the log was to “document every single thing that was said to [her] so [she] could try to figure out why [she] was put on leave,” according to court documents, despite the fact that no one in her new division was involved in the decision to put her on administrative leave.

Painter’s new supervisor also began receiving complaints about her from other employees that she was “violent and dangerous” and emails from her during the evening and in the middle of the night that were “not work-related and nonsensical,” the lawsuit said.

Painter’s supervisor contacted IDOT’s Labor Relations, which recommended Painter go on paid administrative leave. Painter was placed on leave in November 2011, and in December 2012 went to Dr. Terry Killian for another fit-for-duty exam.

Killian determined that Painter was

**ISSUE:** Marijuana  
**BILL:** H. 511  
**VENUE:** Vermont  
**STATUS:** Enacted  
**SIGNIFICANCE:** Legalizes the recreational use of marijuana, eliminating all penalties for possession of one ounce or less by individuals 21 and older.

**ISSUE:** Pregnancy  
**BILL:** Massachusetts Pregnant Workers Fairness Act  
**VENUE:** Massachusetts  
**STATUS:** Enacted  
**SIGNIFICANCE:** Prevents employers from denying new mothers and women who are pregnant reasonable accommodations for their pregnancies and related conditions.
psychiatrically fit for duty, and she returned to work in January 2012. Painter’s colleagues then began submitting complaints about her behavior in the workplace, and her supervisor issued a written reprimand to her for being argumentative.

In April 2012, Painter emailed her union representative and said “for the record, the clock in the small conference room being set to 4:30 p.m. when it was only 4:00 p.m.—that’s a telltale sign for me. It told me everything I need to know,” according to court documents. When asked for clarification about her email, Painter responded with “something’s dead alright—however, I prefer to be a lady and not say what I think is dead.”

The email was treated as a potential threat by IDOT, which contacted the Illinois State Police. Painter was then put on administrative leave, examined by Killian again, and found “psychiatrically unfit for duty as a result of paranoid thinking…and the disruptive behavior which results from her paranoia,” according to court documents.

Painter then filed suit against IDOT for violating the Americans with Disabilities Act (ADA) and subjecting her to unnecessary medical examinations.

The case reached the U.S. Court of Appeals for the Seventh Circuit, which found that IDOT acted reasonably in handling Painter’s case.

The appellate court found that “annoying or inefficient behavior does not justify an examination” but “preventing employees from endangering their co-workers is a business necessity.”

The appellate court determined that the examinations were job related and consistent with business necessity because “inquiries—even multiple inquiries—concerning a worker’s psychiatric health may be permissible if they reflect concern for the safety of other employees and the public at large.”

Based on these findings, the court granted summary judgement to IDOT and dismissed Painter’s case. (Painter v. Illinois Department of Transportation, U.S. Court of Appeals for the Seventh Circuit, No. 16-3187, 2017)

REGULATIONS

DRUG TESTING. The U.S. Department of Transportation (DOT) published a final rule that changes drug testing requirements and adds new substances to its drug testing panel.

The DOT currently requires urine testing for safety-sensitive transportation industry employees who are subject to drug testing under Title 49 Code of Federal Regulations Part 40. Under the new rule, employers will no longer be required to submit blind specimens to the DOT for testing—a requirement that was originally instituted as a quality control measure.

The rule also adds hydrocodone, hydromorphone, oxycodone, and oxymorphone to the DOT’s drug testing panel. The DOT also added methylenedioxymetamphetamine as an initial test, and removed methylenedioxymethylamphetamine as a confirmatory test analyte.

“The opioid crisis is a threat to public safety when it involves safety-sensitive employees involved in the operation of any kind of vehicle or transport,” said U.S. Transportation Secretary Elaine L. Chao in a statement.

LEGISLATION

United States

DATA. U.S. Representative David Cicilline (D-RI) introduced a bill that would require some companies that store Americans’ data to meet specific security and privacy requirements.

The Consumer Privacy Protection Act (H.R. 4081) would require companies that collect and store data on at least 10,000 Americans to implement a “comprehensive consumer privacy and data security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity, and the nature and scope, of the activities of the covered entity,” according to the bill.

Covered data includes Social Security, drivers’ license, and passport numbers; financial account and debit or credit card numbers in combination with PINs; usernames and passwords; and biometric data.

The U.S. attorney general, the U.S. state attorneys general, and the Federal Trade Commission would enforce the requirements in the law, and can fine companies not in compliance at least $16,500.

The bill has nine Democratic cosponsors and has been referred to the House Subcommittee on Crime, Terrorism, Homeland Security, and Investigations.

CONCEALMENT. U.S. Senator Bill Nelson (D-FL) introduced a bill that would require companies to disclose data breaches within 30 days of becoming aware of the breach.

Under the legislation (S. 2179), companies would have to report the breach and any individual who concealed data about the breach could face up to five years in prison.
The bill was drafted in response to the revelation that Uber paid hackers $100,000 to destroy documents and hide evidence of a data breach of more than 57 million records—including customer and driver personally identifiable information.

“We need a strong federal law in place to hold companies truly accountable for failing to safeguard data or inform consumers when that information has been stolen by hackers,” Nelson said in a statement. “Congress can either take action now to pass this long overdue bill or continue to kowtow to special interests who stand in the way of this commonsense proposal.”

Nelson introduced similar legislation in the Senate last year.

The bill has two Democratic cosponsors and has been referred to the Senate Committee on Commerce, Science, and Transportation.

**FIREARMS.** The U.S. House of Representatives passed legislation that would allow people with concealed carry permits to carry firearms across state lines.

The bill (H.R. 38) allows people with concealed carry permits with a valid government-issued photo ID to carry their firearms into another state.

U.S. Representative Richard Hudson (R-NC) sponsored the legislation. He said in a statement that passing the bill was necessary to reflect the “Full Faith and Credit Clause” of the U.S. Constitution, which requires states to recognize the judicial proceedings and documents of other states.

“That’s why a driver’s license is recognized in every state,” Hudson said in a statement. “That’s why if I get married in North Carolina, but I move to Arizona, I’m not a single man again. They recognize that marriage. That’s why divorce decrees are recognized in every state. The concealed carry permit should be recognized the same way.”

H.R. 38 was combined with another provision that will require agencies to report criminal history records to the FBI’s National Instant Criminal Background Check System (NICS).

The measure was created after the First Baptist Church shooting in Sutherland Springs, Texas, where the gunman was able to purchase a firearm because his criminal record was not entered into the NICS prior to the purchase.

Additionally, the bill requires the U.S. Department of Justice to report to Congress the number of times bump stocks are used in crimes. A gunman used bump stocks in a shooting in Las Vegas, which allowed him to make his semi-automatic weapons fire more rapidly and injure more people.

The bill now moves to the U.S. Senate for consideration.
INDUSTRY NEWS | BY FLORA SZATKOWSKI

PARTNERSHIPS AND DEALS

Abloy UK and Bristol Maid supplied Queen Elizabeth Hospital Birmingham with PROTEC2 CLIQ and Traka21 advanced key management systems to improve the security of medicines.

Agent Video Intelligence announced that its innoVi cloud-based video analytics integrate with Amazon Kinesis Video Streams, a service to capture, process, and store video streams for analytics and machine learning.

Allstate Insurance is working with Carpe Data to apply highly predictive online data to claims processing.

Astrophysics Inc. selected Bell and Howell to help increase its service reach and capabilities as the company expands in the United States and Canada.

BIO-key International, Inc., reported that CyberCore Technologies will deploy BIO-key’s ID Director for Windows software authentication platform.

Captis Intelligence will provide Rite Aid with asset protection support service from its corporate office in Los Angeles.

The CNL Software Technology Alliance Program will integrate Jacques Technologies’ IP Communications Systems with the IPSecurityCenter PSIM integrated situation management solution.

Confidex Ltd. was selected to supply smart tickets to Strömma Finland, the operator of Helsinki Card, which provides access to attractions and museums around the capital of Finland.

Cyberbit supplied ISE Systems with a Cyberbit range for its Cybersecurity Training Center in Paris.

Delta Scientific is working with Knight Brothers Pty. Ltd. in Sydney.

BOOTH COMPETITION

B.I.G. ENTERPRISES, INC., inspired both licensed architects and architects-in-training to vie for top prizes in its inaugural 2017 B.I.G. Architectural Booth Design contest. More than 13,000 invitations were sent to current or former students of the 81 universities in the U.S. recognized by either the National Architectural Accrediting Board or the Association of Collegiate Schools of Architecture. Entries came from alumni and undergrads as far away as Malaysia, Colombia, and Albania.

Two award-winning U.S. architects judged the final field of 15 sketches, which were selected based on the buildability of the ideas. The judges praised the combination of indoor and sheltered outdoor space in the submissions. They found that the contest uncovered a broad slice of architectural ideas appropriate to the idea of a guard shelter, whether through a modern approach, a retro vibe, playfulness, or another theme.

The top cash prizes went to Colombian Roberto Caputo for first place, American Benjamin Garcia for second place, and Albanian Frida Vokshi for third place. In the image above, Caputo’s design is second from the left in the top row; Garcia’s design is on the far right on the bottom row.

“We are pleased to offer these new designs to our customers and look forward to discussing an application for each one of them,” says B.I.G. Vice President Dave King.
Australia, to provide security professionals and public space operators with crash-rated vehicle mitigation solutions. DNA and Tosibox will provide DNA real estate customers an advanced data security solution for monitoring building automation systems.

The Electronic Healthcare Network Accreditation Commission is collaborating with Omnisystems, Inc., to offer its accreditation programs, cybersecurity framework, and consultative services to customers in the United Kingdom, the Caribbean, and other markets.

Mphasis selected Fortinet to deliver advanced threat protection and secure data networks in virtualized platform to service its customers.

Galaxy Control Systems enhanced the level of integration between its System Galaxy Access Control and Cloud Concerge products and Schlage NDE and LE wireless locks from Allegion.

Hikvision USA Inc. worked with integrator Holmes Security Systems to provide a security system for The Lodge at Operation Inasmuch men’s shelter in Fayetteville, North Carolina.

ImageWare Systems, Inc., and Secure Channels, Inc., are enhancing the Entertainment Security Operations Center with multifactor biometric authentication.

InfoArmor, Inc., announced that Baird of Milwaukee, Wisconsin, will offer PrivacyArmor identity protection as an employer-sponsored benefit to its employees.

Jumio announced a partnership with Meed to provide remote ID verification services for its package of financial services.

Kastle Systems International announced that its KastlePresence is offered at Cushman & Wakefield’s 1401 Eye Street premier office building in Washington, D.C. It allows staff and tenants to use smartphones to access the building’s perimeter, elevators, and suites.

Kroll announced a partnership with the Center for Internet Security. Savelberg care center in Gouda, The Netherlands, chose the Conview Care solution from Leertouwer. It includes video surveillance, sound and motion detection, and electronic bracelets.

Leidos and SecurityMatters will provide passive monitoring capabilities to enhance cybersecurity for industrial and critical infrastructure networks.

Magal Security Systems, Ltd., will provide integrated security solutions for a major seaport in East Africa as a subcontractor for Toyota Tsusho Corporation. BNP Paribas is using the AESO Security Management Platform from Nedap.

On the Move Systems announced that its subsidiary Robotic Assistance Devices will supply intelligent robotic solutions through Allied Universal to supplement security professionals and drive efficiency.

Park Assist installed its M4 camera-based parking guidance systems at Cherry Creek Shopping Center in Denver, Colorado.

The Louvre in Abu Dhabi is using a Resilient surveillance video storage system solution.

Salient CRGT, Inc., partnered with Kaseware to integrate its Voyager Query for Law Enforcement within the Kaseware investigative case management system.

The Vienna University of Economics and Business worked with Siemens AG Austria to create a networked video system using SeeTec video management software.

Thales announced that Kashing Ltd. is deploying its payShield 9000 hardware security module to secure online e-commerce and mobile point of sale card readers.

TruTag Technologies is providing its TruTag on-dose identity solution to the Daily Wellness Company, a nutraceutical manufacturer. The TruTag solution is covert and edible.

GOVERNMENT CONTRACTS

The Texas Department of Information Resources awarded AT&T a contract to offer managed security services statewide.

Charlotte-Mecklenburg Police Department purchased TASER X2 Smart Weapons from Axon.

BIO-key was selected to provide a biometric solution for the Province of British Columbia.

Bruker will deliver RAID M-100 hand-held chemical detectors to the U.S. National Guard.

Centigon France was selected by SCANIA to protect truck cabins for the Danish Armed Forces.

The U.S. Army Corps of Engineers selected the CH2M-Merrick Joint Venture Bosch Security Systems installed FLEXIDOME IP panoramic 7000 video cameras inside and outside the Serralves Museum of Contemporary Art in Portugal.
to support the Missile Defense Agency’s Ballistic Missile Defense Program with electronic and physical security design.

The Philippines Land Transport Office is issuing 500,000 biometric licenses per month, using a system from DERMALOG.

Design Interactive’s ScreenADAPT, a visual search training program, is being used at the Portland Airport.

The Seagull unmanned surface vessel from Elbit Systems performed mine countermeasures in a joint exercise between the Israeli Navy and the British Royal Navy.

FoxGuard Solutions, Inc., was awarded a grant from the U.S. Department of Defense (DoD) to develop a cybersecurity platform to protect military installations across the world.

Herta will install facial recognition solutions in the city of Phuket, Thailand, as part of a safe city initiative.

MacAulay-Brown, Inc., was awarded a task order to help the U.S. Air Force Research Lab streamline business applications and software across the enterprise.

Milestone Systems’ video management software and Axis Communications’ network video cameras are helping protect Las Ramblas in Cayala City, Guatemala. EMC Isilon servers provide the data storage.

MSA Safety provided state-of-the-art G1 self-contained breathing apparatus to the Chicago Fire Department.

Orion Communications announced that the Massachusetts State Police selected its AgencyWeb solution to streamline scheduling, deployment of resources, training, supply management, and asset tracking.

Sullivan County Emergency Communications District in Tennessee transitioned to PowerPhone’s Total Response solution.

RADWIN announced that Antwerp Police in Belgium chose its JET Point-to-Multipoint solutions to build a video surveillance network.

The Brazilian Ministry of Education is using the ANDRE Advanced Nearfield Detection Receiver from Research Electronics International to detect cheating at standardized testing.

Siklu Inc. announced that its Multi-Haul radios were selected by Wichita, Kansas, to provide wireless connectivity for cameras deployed in the city’s Old Town district.

Threat Sketch was awarded a contract from the National Institute for Hometown Security and the U.S. Department of Homeland Security to help develop innovative solutions for the critical infrastructure community.

Wireless video experts xG Technology, Inc., will supply hand-held intelligence, surveillance, and reconnaissance devices to the U.S. Army.

AWARDS AND CERTIFICATIONS

Hosting company 3W Infra achieved compliance with ISO 27001 and PCI-DSS standards, according to audit company Noordbeek B.V.

A+ Technology & Security Solutions was named 2017 Education Partner of the Year by Axis Communications.

Akoustis Technologies, Inc., announced that its wafer fabrication facility in Canandaigua, New York, achieved ISO 9001:2015 certification. It also received new patents related to its piezoelectric materials, resonators, RF

**STRATEGIC MOVES IN THE NEWS**

<table>
<thead>
<tr>
<th>WHO</th>
<th>WHAT</th>
<th>OF/WITH</th>
<th>RESULT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Convergint Technologies</td>
<td>ACQUISITION</td>
<td>Genesis Security Systems</td>
<td>The acquisition will bring additional electronic security systems and utilities market expertise to Convergint’s customers.</td>
</tr>
<tr>
<td>TruTag Technologies</td>
<td>STRATEGIC PARTNERSHIP</td>
<td>Sumitomo Corporation of Americas</td>
<td>The partnership will adapt TruTag’s technology for product identity, traceability, and supply chain management of various Sumitomo divisions worldwide.</td>
</tr>
<tr>
<td>DC Capital Partners Management, LP</td>
<td>ACQUISITION</td>
<td>Janus Global Operations</td>
<td>Collaboration with partner companies in the DC Capital portfolio will allow Janus to expand its capabilities to current clients and reach out to new clients.</td>
</tr>
<tr>
<td>Arteco</td>
<td>PARTNERSHIP</td>
<td>Bosch Security Systems</td>
<td>Integration between Arteco’s NEXT video event management system and Bosch technologies will deliver advanced functionality to their customers.</td>
</tr>
</tbody>
</table>
filters, and their applications. Arxsy Software Orchestrated Storage is now a Milestone Certified Solution. Convergint Technologies was named 2017 National Systems Integrator of the Year by Axis Communications. Detection Technology was granted ISO 9001:2015 and ISO 14001:2015 certification.

Hanwha Techwin’s high-performance chipset Wisenet 5 won the Grand Prize at the High-Tech Safety Industry Product and Technology Awards 2017. G4S Secure Solutions (USA) was named Outstanding Philanthropic Corporation by the Association of Fundraising Professionals of Palm Beach County. IdeaScale announced its FedRAMP authorization. Lieberman Software Corporation announced that its Rapid Enterprise Defense Identity Management is certified for Microsoft Azure Government.

Mimiccast Limited was named one of the Top Places to Work in Massachusetts by The Boston Globe. Little Caesars Arena, home of the Detroit Red Wings and Detroit Pistons, received SAFETY Act Certification from the U.S. Department of Homeland Security. The arena is managed and operated by Olympia Entertainment.

The VARIO2 IP Hybrid Illuminator from Raytec won an award for Innovative Achievement (Video Surveillance) at the Detektor International Awards 2017. Rohde & Schwarz achieved U.S. Transportation Security Administration certification for its R&S QPS200 Security Scanner.

RSA announced that its NetWitness Suite was added to the U.S. Department of Defense Information Network Approved Product List. Cloudera named Securonix Inc. the Cloudera APAC Technology Partner of the Year.

SmartMetric announced that its biometric card is protected by five new patents. Suprema was recognized with the Best Product Award in the ID & Access Control category at the Detektor Awards. VVIPRE Security won the Channel-nomics Innovation Award. Votiro received the Common Criteria Certification from the Australian Signals Directorate following evaluation by BAE Systems.

ANNOUNCEMENTS

Alarm Lock Systems, a division of NAPCO, launched a new website at www.alarmlock.com. The Alliance for Cyber Risk Governance introduced its risk framework initiative at its inaugural conference. The alliance plans to establish four working groups responsible for expanding on the initial recommendations. Former Massachusetts Governor Michael Dukakis and Tuan Nguyen founded the Artificial Intelligence World Society to foster the ethical development, implementation, and advancement of artificial intelligence.

Quebec’s Bureau de la Sécurité Privée launched a new website at www.bspquebec.ca/en as an essential reference portal for the private security industry. Cisco and INTERPOL agreed to share threat intelligence as the first step in jointly fighting cybercrime.

The Cloud Security Alliance released the CSA Code of Conduct for GDPR Compliance, which provides guidance in complying with the European General Data Protection Regulation. Contemporary Services Corporation renamed its Las Vegas employee training center in honor of an employee, Erick Silva, who was fatally shot during the attack on the Route 91 Harvest Festival.

Datacenter.com announced the official opening of its Amsterdam flagship colocation data center. Ernst & Young LLP acquired E-STET, which will join its Fraud Investigation and Dispute Services. Exterro Inc. announced a new educational website to educate lawyers on the e-discovery implications within the Federal Rules of Civil Procedure. The Special Investigations Unit of the International Centre for Sport Security established a confidential Sport Integrity Hotline to help athletes, fans, and others report misconduct and sport integrity issues in the United States and Canada.

Karamba Security was invited to join the Automotive-Information and Sharing Analysis Center (Auto-ISAC). KOLOGIK acquired the assets of COPsync of Dallas, Texas, to create a law enforcement regional data sharing network across Texas, Louisiana, and Mississippi.

The National Electrical Manufacturers Association and the Industrial Internet Consortium formed a formal liaison to advance the Industrial Internet of Things. Midpoint Security is offering a free edition of CredoID access control software, which is compatible with HID VertX controllers, Edge IP readers, Mercury controllers, Suprema biometric IP, and wireless Aperio locks by Assa Abloy.

The mobotour team is seeking three individuals to serve on the company’s advisory board—one in middle school, one in high school, and one in college. Learn more at mobotour.com/mobotour_advisoryboard_contest.

Nuctech launched a new branch in Rotterdam, The Netherlands. The Ministry of Community Safety and Correctional Services in Ontario, Canada, used 16 ODSecurity Soter RS Body Scanners to perform 139,600 scans in 2017, yielding 4,774 positive scans that uncovered mobile phones, weapons, and drugs.


Traffic & Parking Control Company opened a Minnesota Service Center in White Bear Lake, Minnesota.
CODA OCTOPUS GROUP, INC., of Orlando, Florida, launched the first product in its fourth-generation range of sonars, the Echoscope4G Surface. The patented Real Time 3D sonar enables vision, mapping, and measurement in real time in low- or zero-visibility conditions under water. Designed for nearly plug-and-play ease of use for shallow water operational needs not to exceed 20 meters (66 feet) water depth, the unit is 50 percent lighter and 40 percent smaller than the earlier product line. It uses 30 percent less power without compromising real-time 3D image and mapping fidelity, performance, or capability. 302

New infinias access control 6.2 software from 3XLOGIC, INC., of Westminster, Colorado, offers seamless integration with 3xLOGIC VIGIL video appliances and more. Users can view live or playback video for a specific access control event or view live video for a specific door. Users can also change video resolution, take a snapshot, and search playback video for any event. The software now supports 3xLOGIC’s Site Access mobile app for viewing video and managing events, doors, and people. From a mobile device on all versions of infinias, end users can view video by door, suspend people, momentarily unlock doors, receive push notifications, and review six months of past notifications. 301

Chicago-based OCCLY LLC offers a wearable Body Cam Alarm System, featuring four cameras that capture nearly 280 degrees around a worker to provide employee safety and protection. The system continuously records an employee’s environment, compressing, encrypting, and storing data on the Occly hardware. In the event of an emergency, the wearer presses the panic button or triggers another sensor built into the device, an alarm begins, and video and audio information is sent in real time to The Occly Monitoring Service. Professional monitoring representatives assess the situation using images from before the alarm, as well as those received in real time. 303
Developed specifically for airport applications, the Horton ControlFlow™ One-Way Revolving Door protects against security breaches in high-volume traffic areas. Horton’s patented Object Detection Technology uses a light curtain and photo-reflective sensors to scan for objects left behind and to prevent objects from passing into the secure area.
FOUR CHALLENGES FACING AVIATION SECURITY

ANTHONY MCGINTY, CPP, IS A SENIOR INTELLIGENCE ANALYST WITH CSRA INC., CONTRACTED TO LOS ANGELES INTERNATIONAL AIRPORT. HE IS A MEMBER OF THE ASIS GLOBAL TERRORISM, POLITICAL INSTABILITY, AND INTERNATIONAL CRIME COUNCIL.

1. AIRPORTS AS CITIES. Traditional city problems are finding their way into airports—the homeless, the mentally ill, drug abuse, petty and complex crime, and civil disobedience. For law enforcement and security agencies, the challenge is to simultaneously perform first-responder duties while identifying high-consequence threats to aviation operations. Both require specific, distinct skill sets. Security directors need to balance assets, personnel, and operations to mitigate both public disorder and homeland security risks.

2. INTERNATIONAL TERRORISM. Commercial aviation will remain an attractive target for militant groups and extremists. The public side of airports—curbside to security screening—is vulnerable to an array of terrorist attacks, including active shooters, luggage filled with explosives, weaponized drones, and vehicle ramming. Thousands of militants, technically proficient and ideologically motivated, who are returning from the failing ISIS caliphate may regroup under new flags, join al Qaeda affiliates, or act independently.

3. IN-FLIGHT DISRUPTIONS. On a weekly basis, media reports and Internet videos display the latest outrage inside aircraft cabins—brawling, drunken rants, sexual assaults, and defying flight attendants. This trend of in-flight disputes and violence at 35,000 feet is potentially dangerous. Short of placing a security officer on board, solutions may involve institutional changes in the flight crew-to-passenger relationship. For example, instances of human traffickers using commercial airlines are so common now that flight crews are being trained to spot indicators and act. This is a further example of the changing role of flight crews from comforters to enforcers.

4. INSIDER THREAT. Terrorist groups may enlist airport employees to circumvent security screening—especially employees with direct access to aircraft. Employees have also smuggled drugs, weapons, and other contraband. Just one radicalized or disgruntled employee can commit an act that leads to a catastrophic incident, which makes addressing insider threats a priority. Airports and airlines are implementing their own strategies to mitigate this threat. Mostly, this effort has involved security screening of all—or select—employees prior to entering restricted zones. Technology may support this effort as well. New analytics capabilities embedded in video and access control systems can provide a sophisticated surveillance tool. Self-policing with a rigorous, internal “See Something, Say Something” effort is essential.
Together we can

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

Supporting Families Across America

For product info #21 securitymgmt.hotims.com
The Security Professionals’ first choice for today’s security infrastructure, from one room to multi-location complexes around the world. Our reputation is based on a time-honored tradition of rock-solid quality, premium reliability and integrity of DSX and our network of factory-trained, authorized dealers and support.

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

DSX STANDARD SYSTEMS FEATURES INCLUDE:

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